Ryedale District Council

Internal Audit Annual Report

2015/16

Audit Manager:	Stuart Cutts
Head of Internal Audit:	Max Thomas
Circulation List:	Members of the Overview and Scrutiny Committee Chief Executive Finance Manager (S151 Officer)
Date:	28 July 2016

Veritau
Assurance Services for the Public Sector

Background

1 The Accounts and Audit Regulations 2015 require the council to have an effective internal audit service that complies with public sector internal audit standards. The Chartered Institute of Public Finance and Accountancy (CIPFA) is responsible for setting those standards and together with other bodies responsible for internal audit standards in the public sector has agreed common standards known as the Public Sector Internal Audit Standards (PSIAS)

2 As well as providing a definition of internal auditing, the PSIAS detail the code of ethics for internal auditors and provide quality criteria against which performance can be evaluated. Since the standards were adopted CIPFA has also issued further guidance in the form of an application note. The application note includes a checklist to assist internal audit practitioners to review and update working practices.

3 In connection with reporting, the relevant PSIAS standard (2450) states that the Chief Audit Executive (CAE)[1] should provide an annual report to the board[2]. The report should include:

(a) details of the scope of the work undertaken and the time period to which the opinion refers (together with disclosure of any restrictions in the scope of that work)

(b) a summary of the audit work from which the opinion is derived (including details of the reliance placed on the work of other assurance bodies)

(c) an opinion on the overall adequacy and effectiveness of the organisation's governance, risk and control framework (i.e. the control environment)

(d) disclosure of any qualifications to that opinion, together with the reasons for that qualification

(e) details of any issues which the CAE judges are of particular relevance to the preparation of the Annual Governance Statement

(f) a statement on conformance with the PSIAS and the results of the internal audit Quality Assurance and Improvement Programme

4 During the year to 31 March 2016, the Council's internal audit service was provided by Veritau North Yorkshire Limited, which is part of the Veritau Group.

Internal audit work carried out in 2015/16

5 During 2015/16, internal audit work was carried out across the full range of the council's activities. The main areas of internal audit activity included:

- **Strategic risk register** – We have completed three audits in 2015/16. For Business Continuity, the Council's framework is developing and so we provided further guidance and advice on areas to focus on in the future. For ICT disaster recovery, our review of arrangements concluded with an overall 'Reasonable Assurance' rating. We have also reviewed the council's arrangements to combat fraud and corruption risks against the CIPFA code of

[1] The PSIAS refers to Chief Audit Executive. This is defined in RDCs charter as the Head of Internal Audit.
[2] The PSIAS refers to the board. This is taken in RDCs charter as the Overview and Scrutiny Committee.

practice. The findings from these three audits are explained in more detail in Appendix 2 to this report.

- **Financial systems** - work in this area provides assurance to the council on the adequacy and effectiveness of financial system controls. We have reviewed seven key financial systems. On the whole the council has relatively strong arrangements with two of the audits being given 'High Assurance; opinions and four of the audits 'Substantial Assurance'. With Payroll we found a number of control weaknesses and therefore gave a 'Reasonable Assurance' rating. Further information on these audits is included in Appendix 2. The weaknesses in respect of payroll have been referred to in the Audit Opinion and Assurance Statement in paragraph 13.

- **Regularity audits** – we have completed four audits during the year covering a number of different operational areas. We have identified a number of areas in these audits where the council can make improvements. The audits on Contract Management (Corporate Arrangements) and Sickness Absence were both given 'Reasonable Assurance' opinions. We also provided some specific feedback following our review of the Leisure Services contract. Our review of Risk Management identified a number of control weaknesses and was therefore given a 'Limited Assurance' rating. The findings from all four reports are explained in further detail in Appendix 2 to this report. The weaknesses highlighted as a result of the Risk Management audit have been referred to in the Audit Opinion and Assurance Statement in paragraph 13.

- **Technical / projects** - our work covered five separate areas, four of which we have previously reported to this Committee. Three audits were given 'Limited Assurance' opinions. One of these audits, Payment Credit Industry Data Security Standard (PCI DSS), is explained in further detail in Appendix 2 to this report. The other two audits given 'Limited Assurance' opinions are included for information in Appendix 3. In respect of the audit on Data Protection and Security, the Council has made a number of improvements since our audit was reported.

- **Follow up** - it is important that agreed actions are followed up to ensure that they have been implemented. Veritau follow up agreed actions on a regular basis, taking account of the timescales previously agreed with management for implementation. Our work shows that progress has been made by management during the year to address previously identified control weaknesses. However there are specific areas referred to in Appendix 2 (on Payroll and PCI DSS) where agreed actions had not been completed and management are therefore planning to ensure these are addressed in 2016/17.

6 Appendix 1 provides a summary of the audit work carried out in the year, and the opinions given for each completed audit. Further details of the key findings and agreed management actions for each audit are given in Appendices 2 and 3. The opinions and priority rankings used by Veritau are detailed in Appendix 4.

7 We agreed with officers to cancel the 2015/16 proposed work on Performance Management arrangements and Data Quality. This allowed for additional time to be provided to fully review and report the issues from the other work in the Audit plan.

Compliance with Public Sector Internal Audit Standards (PSIAS)

8 The work of internal audit has been undertaken in accordance with the PSIAS. Veritau has an established Quality Assurance and Improvement Programme.

9 The programme includes ongoing monitoring of the performance of the internal audit activity. Ongoing monitoring is an integral part of the day-to-day supervision, review and measurement of the internal audit activity. All audit work is reviewed by senior staff and a sample of work is also subject to internal peer review. All reports are reviewed by Audit Managers prior to being issued to officers. Post audit customer satisfaction surveys are issued after all assignments. In addition, senior management in each client organisation are asked to complete an annual survey on the overall quality of the service provided by Veritau.

10 External assessments must be conducted at least once every five years by a qualified, independent assessor or assessment team from outside the organisation. An external assessment was carried out in 2014 by the South West Audit Partnership (SWAP). The outcome from the review demonstrated that the service provided by Veritau conformed to the International Standards for the Professional Practice of Internal Auditing.

11 Further details about the 2016 Quality Assurance and Improvement Programme are shown in Appendix 5.

Audit Opinion and Assurance Statement

12 The overall opinion of the Head of Internal Audit on the governance, risk management, and control framework operating in the Council is that it provides **Reasonable Assurance**. There are no qualifications to that opinion. No reliance was placed on the work of other assurance bodies in reaching this opinion.

13 Although a reasonable assurance opinion can be given, we are aware of some specific weaknesses in the control environment which have been identified in respect of the systems for Payroll and Risk Management. The council should consider whether it feels these two areas are required for inclusion in the council's Annual Governance Statement.

Max Thomas
Director and Head of Internal Audit
Veritau Ltd

28 July 2016

Appendix 1

Audit	Status	Assurance Level	Audit Committee
Strategic Risk Register			
Business Continuity	**Completed**	**No opinion given**	**July 2016**
Disaster Recovery	**Completed**	**Reasonable Assurance**	**July 2016**
Fraud and Corruption	**Completed**	**No opinion given**	**July 2016**
Performance Management arrangements and Data Quality	Cancelled	**-**	**-**
Financial Systems			
Housing Benefits	**Completed**	**Substantial Assurance**	**April 2016**
Payroll	**Completed**	**Reasonable Assurance**	**July 2016**
Council Tax / NNDR	**Completed**	**High Assurance**	**January 2016**
Sundry Debt Recovery	**Completed**	**Substantial Assurance**	**April 2016**
Creditors	**Completed**	**Substantial Assurance**	**July 2016**
General Ledger	**Completed**	**High Assurance**	**July 2016**
Budgetary Management	**Completed**	**Substantial Assurance**	**July 2016**
Regularity Audits			
Risk Management	**Completed**	**Limited Assurance**	**July 2016**
Contract Management – Corporate Arrangements	**Completed**	**Reasonable Assurance**	**July 2016**
Contract Management – Leisure Services	**Completed**	**No opinion given**	**July 2016**
Human Resources – Sickness Absence	**Completed**	**Reasonable Assurance**	**July 2016**
Technical/Project Audits			
Projects - Payroll budget monitoring development	**Completed**	**No opinion given**	**November 2015**
Projects - Cash Payments Ryedale House	**Completed**	**No opinion given**	**November 2015**
Server Rooms security	**Completed**	**Limited Assurance**	**January 2016**
Data Protection and security	**Completed**	**Limited Assurance**	**November 2015**
Payment Card Industry Data Security Standard	**Completed**	**Limited Assurance**	**July 2016**
Follow-Ups	**Completed**	**N/A**	

Appendix 2

Summary of Key Issues from audits completed and final reports issued/agreed; not previously reported to Committee

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
Business Continuity	No opinion	The council's responsibilities for business continuity follow from the Civil Contingencies Act 2004 which states that councils should ensure that they can continue to deliver their functions in an emergency 'so far as is reasonably practicable'. In addition to these statutory requirements, there are service and business reasons for why the council needs to have comprehensive and robust business continuity plans in place. We reviewed the council's arrangements for ensuring effective business continuity arrangements were in place throughout the organisation.	April 2016	The council had identified that business continuity plans needed to be re-written as the current plans were out of date and incomplete. Since November 2015, the council has employed an Emergency Planning Officer from North Yorkshire County Council (NYCC) one day a week to help develop new business continuity plans and procedures. So whilst some work has been undertaken, the council's business continuity arrangements are still evolving. We met with officers and discussed current and proposed arrangements. We noted that the experiences from the flooding and power outages in December 2015 were being captured to help influence future business continuity arrangements. A memorandum was issued for officers offering further guidance on some areas for consideration in 2016/17 including the need to effectively integrate business continuity within the council (with areas such as service delivery, risk management and ICT disaster recovery) and to ensure the future policy becomes fully embedded throughout the organisation.	At the time of writing the report, a draft of the business continuity policy had been written and was being reviewed by key individuals with a view to a final policy on business continuity being issued in 2016/17. The council is to continue to develop arrangements on business continuity in 2016/17.
Disaster Recovery	Reasonable Assurance	ICT disaster recovery is the process of recovering information technology systems and services. Disaster recovery (DR) forms part	June 2016	**Strengths** The council has developed documentation to guide disaster recovery. The IT Infrastructure Manager has a thorough understanding of	Some initial steps are to be considered by management. Longer term improvements to

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
		of wider business continuity planning arrangements intended to restore normal business functionality as quickly as is required by service areas. Effective IT disaster recovery plans should provide for a structured and timely recovery of services in the event of an incident, and should help reduce disruption to a pre-determined acceptable and managed level. Our review examined whether: • the council had developed documents and maintained an ICT DR plan; • DR roles and responsibilities were clearly defined; • DR plans were tested • System restoration was appropriately prioritised, and • Data was available for restoration.		the council's network, server roles and back-up arrangements. **Areas for improvement** The council has not carried out a full test of ICT disaster recovery arrangements for some time. The council's overall level of resilience can only be judged by carrying out comprehensive testing of a 'true' disaster situation. The council has back-ups on replicated servers at its depot and also tape back-ups held in a safe in the garage adjacent to Ryedale House. However, the back-ups are not routinely tested to ensure that they would function correctly and data would be available after a disaster. If Ryedale House was inaccessible, tape back-ups in the neighbouring garage could also be inaccessible. The fire-proof safe is also an antique model, which does not have a rating for data. The ICT Services Disaster Recovery Plan has not been approved by senior management. The DR Plan and the reconciliation of systems and servers both include information on the priority of service restoration, but don't include the background detail showing how the council arrived at these priorities. The prioritisation of services for restoration is derived from the corporate Business Continuity Plan, which is in need of revision.	arrangements are to be considered as part of the council's 'Towards 2020' efficiency programme in 2016/17.

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
Fraud and Corruption Arrangements	No opinion	In 2014, CIPFA published a Code of Practice on managing the risks of fraud and corruption. The Code provides a high level set of principles that can be applied to any public sector organisation. The audit reviewed the counter fraud arrangements at the council against the five principles contained in the CIPFA Code of Practice (and the detailed guidance notes) which are that: • responsibility of the governing body for countering fraud and corruption is acknowledged • relevant fraud and corruption risks are identified • an appropriate counter fraud and corruption strategy has been developed and implemented • resources are provided to implement the strategy • action is taken in response to fraud and corruption. It is important that councils tailor their approach to implementing the principles and make the best use of available resources.	May 2016	**Strengths** The management team at the council take fraud matters seriously. There have been a number of instances where this has led to decisive action being taken on particular cases. Fraud is also highlighted as a risk on the council's corporate risk register. There has been close working with Veritau's fraud team on reactive and proactive fraud issues. This close working and serious focus on fraud matters gives the council a good base upon which to make further improvements. **Areas for improvement** The council has a 'Counter Fraud and Corruption Strategy' which has been recognised as being out of date. An update to this document is being completed. A key action once the overall strategy is agreed and finalised is to complete fraud awareness training throughout the council. The Code highlights the benefit of an annual fraud risk assessment governed by a formal risk methodology. The risk assessment exercise is best supported by work such as fraud risk workshops in departments, comparing risks with other similar organisations and involving specialists to help conduct the fraud risk review. The Council did not complete such a formal exercise in 2015/16 although fraud risk has been considered as part of the council's general risk management processes. The Code highlights a number of policies	We have agreed a fraud related programme of work with Veritau to help develop the Counter Fraud policy framework. Each of the areas referred to in the report will be addressed in 2016/17.

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
				covering a variety of areas. The need for robust up-to-date policies to cover key requirements of the CIPFA code is recognised by management. Whilst all of these areas are covered by existing council policies, many have not been formally reviewed for some time. The council also does not have an assurance/compliance framework to provide confirmation all staff are aware of/ have acknowledged responsibilities for each policy.	
Payroll	Reasonable Assurance	The council's payroll is processed by City of York Council (CYC) and so the arrangements operated by the council involve some 'in-house' processes alongside the work undertaken by CYC. We specifically covered the procedures and controls within the payroll system that ensured: • Payments are only made to valid employees at agreed rates of pay and any additional payments were accurate and appropriately authorised • The terms of the service level agreement with the payroll provider are fulfilled and regular and accurate management information is produced. • Calculations of deductions were at the correct and authorised rate • Payroll transactions are	June 2016	**Strengths** The payroll information received from CYC is accurately reflected in the council's ledger. Changes to employment details are appropriately authorised, notified to CYC and relevant supporting information is held on file. Mileage and other travel and subsistence claims are checked and authorised prior to being paid. **Areas for improvement** Our payroll audit in 2014/15 identified there was no service level agreement (SLA) in place with CYC for carrying out the payroll service. There is now a SLA in place but it is still in draft. The council is currently discussing with CYC to expand use of the payroll system to incorporate self service functions. These discussions will provide a good opportunity to further clarify the service provided by CYC and enable the council to agree a clear SLA which will allow for effective performance monitoring of the contract.	Management are working with CYC to update the SLA as part of the roll out of the self service discussions. The RDC HR Manager is to speak with HR managers at CYC and NYCC to establish how they remunerate shift workers to help identify ways of replacing the multipliers system. Salary advance information will be recorded electronically on one document. Although the sums involved are relatively small we agreed there is a need for a robust process in place which is regularly monitored. Other matters will also be addressed in 2016/17.

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
		accurately reflected in the council's accounts. Our work on Payroll in 2014/15 highlighted a number of weaknesses which were reported to Members in November 2014. We recommended these weaknesses in the Payroll control environment were included in the council's Annual Governance Statement in July 2015.		As in 2014/15, we again found issues with multiplier payments for employees who work outside of normal office hours. Uncertainty in the handling of the calculations for multipliers when applied to bank holiday payments may have resulted in some employees being paid incorrectly. A review of the procedure for the payment and recovery of salary advances found that financial records were inconsistent, and there are weak authorisation controls in place for authorising payments. There were also delays in the recovery of some salary advances. There were also some other areas highlighted in the 2014/15 report where little or no action had been taken. These findings will remain open and will be followed up again in 2016/17.	
Creditors	Substantial Assurance	We reviewed the processes and controls for ordering supplies and services. The audit also examined the system for processing creditor payments to ensure payments were only made for valid invoices, the amounts were correct and payments were made within the required timescales. We used computer audit software to support our work and also reviewed council expenditure in 2015/16 to help identify potential duplicate payments.	May 2016	**Strengths** No issues were found with the expenditure that was being made. Payments are made for valid invoices and the correct amount. Use of the purchasing system for the majority of council expenditure ensures goods are receipted before payments are made. We concluded that overall the creditors system appeared to be operating effectively. **Areas for improvement** Invoices are still being received that do not have a purchase order, despite them not being utility or other payments that are	We will reiterate the proper process to be followed in line with Financial Regulations through an email to budget managers. The current ordering process will also be reviewed as part of the 'Towards 2020' efficiency programme. For potential duplicate payments and splitting of invoices then Veritau will help provide us periodic assurance

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
				exempt from these financial regulations. There are no specific controls in place to identify duplicate payments although most duplicate invoices will be identified by officers. However, it is still possible for some to be paid in error. Our work identified 7 invoices which may be duplicate payments (amounting to about £9k) which were passed to the accounts payable officer for further investigation. We also highlighted a potential control gap in respect of splitting of invoices. No such payments were identified during this review. Requests to change a supplier's bank details may be received by any section, not just Finance. It is important that all sections are aware of the need to verify the validity of such requests. We found there are multiple duplicate suppliers on the system as well as multiple addresses for the same supplier.	using their computer audit software to help ensure these potential risks do not materialise. We will review the quality of information input to the financial system and give additional training where required. Where there is inaccurate data in the creditors system then this will be cleansed.
General Ledger	High Assurance	The purpose of this audit was to provide assurance to management that: • Responsibilities and processes for journal entries are appropriately defined and followed. • Cash accounts are regularly reconciled with the appropriate bank accounts. • Control accounts are regularly reconciled.	April 2016	**Strengths** There are established controls and procedures relating to journals which ensure all relevant entries are authorised prior to posting. Any items coded to an incorrect ledger code are automatically sent to a suspense account. The suspense account is monitored and is cleared out on a regular basis. Debtors and creditors control accounts are reconciled daily and other control accounts reconciled monthly. When variations between	

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
		• Suspense accounts are regularly cleared.		systems are flagged up during reconciliations these are investigated appropriately. Any differences between the systems are documented. **Areas for improvement** No significant issues identified.	
Budgetary Management	Substantial Assurance	Management of the council's budgets is a key internal control. Effective budgetary preparation and monitoring will enable the council to be assured the overall financial position is being properly managed, value is being obtained from expenditure and also help support the delivery of the future aims and objectives of the council. Our work involved meeting with officers who are responsible for the monitoring and review of the budget. We reviewed the budget procedures and controls to establish whether: • Procedures were being operated in accordance with the Financial Regulations • Budgetary monitoring, review and reporting procedures were successfully assisting managers to work within their set budget. • The quality of budgetary information is sufficient for future requirements.	May 2016	**Strengths** Budget holders found the monthly budget reports a useful and user friendly way to monitor their budgets. They were happy with the assistance they received from the Finance team when dealing with budget issues. Procedures being operated were consistent to those in the council's financial regulations. **Areas for improvement** It was felt some additional training would be helpful to maximise the knowledge and value budget holders could obtain from the system. We also noted a lack of guidance notes. There are also opportunities for more information to be provided to some budget holders on grants and expenditure that is recharged from other areas.	In 2016/17, the s151 officer is planning further training with budget holders and moving them onto the web based version of the software for GL enquiries. The s151 officer is to discuss with budget holders in respect of the extra information requested.

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
Risk Management	Limited Assurance	Risk management is a critical part of the strategic management of any organisation. It should be a continuous and developing process which runs throughout the organisation, methodically addressing all risks and opportunities surrounding past, present and future activities. The purpose of this audit was to review the council's risk management procedures and ensure that: • All identified risks are assessed and prioritised at corporate and service levels and are fully integrated into existing management arrangements. • Identified risks are assessed regularly, appropriately and effectively. • Appropriate processes are in place to ensure the effective management of the identified risks.	May 2016	**Strengths** A training session was held with managers in December to help start to re-energise and communicate the council's expectations in respect of risk management. Work is currently underway in updating and populating service risk registers. **Areas for improvement** Significant work is required in some areas in order to bring Covalent up to date. Many corporate risks show no evidence of being monitored or controlled, and they are not ranked in order of priority. Service risks, project risks and significant partnership risks all show a lack of evidence of monitoring or control. Covalent has not been populated with mitigating controls and actions.	It was acknowledged by senior management the consistent operation of effective risk management has not happened. One of the projects which forms part of the transformation programme is a re-design of the use of Covalent. Corporate risks will be prioritised on Covalent and there will be a review of the risks included. Mitigating actions will be added where appropriate. Following the launch of the web-based browser for Covalent, Management Team will review corporate risks monthly and in response to any factors arising. A programme of priority projects will be maintained on Covalent together with the associated risk plans. Partnerships will be linked to the relevant service delivery plans with mitigating actions for each.
Contract Management Corporate Arrangements	Reasonable Assurance	The council spends a significant amount of money with third party providers. Good contract management will help ensure	June 2016	**Strengths** Contract management across the council is the responsibility of individual contract managers. Some contracts are being	An updated and complete Contracts Register will be prepared and maintained on the Covalent system.

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
		compliance with performance criteria and reduce the risk of fraud. It will also help to maximise the value that is obtained to the council and the public from the supplier relationship. The audit reviewed the arrangements in place to ensure that: • The council's contract management procedures are being operated in line with expected policy and procedures; and • The contract management arrangements are effective across the organisation. We reviewed a sample of contracts and discussed the application of the contract management procedures with officers.		managed well with contract managers showing a good understanding of key responsibilities such as relationship management and the monitoring of costs. **Areas for improvement** There is no corporate monitoring of contracts. We would expect a form of 'assurance mechanism' in place for the council to be satisfied effective contract management is taking place across the organisation. There is no complete and up to date list of council contracts held within one register. Whilst a contracts register is maintained for publication this register is incomplete and out of date. There is no central repository for contracts and in some cases contract managers did not hold a copy of the contract they were responsible for managing. There are no corporate policies, procedures, guidance or training in place to support good quality (and proportionate) contract management. Contract management is a skill and not all managers will have the same level of knowledge and experience.	Responsible officers for each contract will be assigned. All contracts on the new register on Covalent will be assessed for significance. Those that are significant contracts and therefore are a high risk to the council will have a risk register included on Covalent. A working group will be developed through service unit managers and heads of service. This group will review high risk contracts. Corporate policies and guidance for contract management will be developed to support managers in their contract management responsibilities.
Contract Management Leisure Services	No opinion	The council appointed Sports and Leisure Management (operating as Everyone Active) in November 2014 to deliver its leisure services. The Corporate Director recognised the potential risks involved in the new Leisure Services contract and	May 2016	We noted that performance management arrangements are good, with a significant amount of information received and further information available as required. We highlighted a small number of potential improvements to current performance measures.	

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
		requested a review of the arrangements in place with Everyone Active. The objective of the review was to help identify how contractual performance management arrangements could be strengthened and improved.		To ensure the contract management arrangements focus on the areas of greatest risk we recommend the contract risks were formally evaluated and recorded in a risk register. An up to date risk register will help ensure the contract is being managed effectively and proportionately. At present the council is obtaining some assurance through reported statistics and on the spot checks. The development of a comprehensive assurance framework will allow the council to obtain assurance over the provision of the service. We suggested the focus should be on ensuring there are effective processes in place rather than conducting detailed compliance tests. For example, the review of swimming pool temperature monitoring should focus on whether the provider has a process in place to carry out temperature monitoring (and checking the outcomes/compliance of that policy) as opposed to direct testing by officers.	
Human Resources – Sickness Absence	Reasonable Assurance	The purpose of this audit was to provide assurance that effective policies and processes are in place for managing sickness absence.	May 2016	**Strengths** Our work found sickness absence data is being correctly and accurately recorded for both monitoring and payroll purposes. **Areas for improvement** Application of the Absence Management policy is not consistent across all service areas. As an example, we found return to work (RTW) interviews are not routinely being carried out in some cases. Some records for	Discussions are in progress with the HR/payroll system provider to help maximise the use of the system to support sickness absence case management. The processes involved are being reviewed along with other HR processes as part of the T2020 programme. Trigger points in the Attendance Management

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
				RTW interviews are incomplete in some service areas. Effective management of sickness absences was also being further hindered by a lack of accurate and timely information for managers about trigger points being reached. Instead managers were relying on their own records. It has also been several years since attendance management training has been provided.	Policy will be reviewed. All Managers will be reminded of the need to complete Return To Work interviews. Absence Management refresher training will be provided to Managers to tie in with training arising from the use of iTrent.
Payment Card Industry Data Security Standard	Limited Assurance	The Payment Card Industry Data Security Standard (PCI DSS) is an international standard mandated by the five major card providers. They have collectively adopted the PCI DSS as the requirement for all organisations which process, store or transmit payment cardholder data. Payments accepted using any debit, credit, or pre-paid card from these providers are subject to the standard. The council is required to follow the necessary parts of the standard to be in a position to confirm security over the data to which it is responsible. Compliance with the standard is not straightforward. An earlier audit report issued in July 2015 identified a number of areas requiring improvement.	July 2016	**Strengths** There has been some limited progress made in addressing the findings from the previous PCI DSS audit. **Areas for improvement** There are still a number of key issues that need to be addressed before the council is compliant with the PCI DSS requirements. The lack of progress has not been helped by the absence of an effective action plan. Such a plan would help by assigning roles, responsibilities and timescales for each task. In areas where some progress has been achieved (e.g. obtaining compliance assurances from third parties and identifying all processes subject to PCI DSS) then further work is still required. The council does not currently have any procedure notes in place for processing payments.	

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
				The council also needs to identify the level of relevant transactions and complete and submit the PCI DSS compliance questionnaire. In the future, whenever the council makes an operational decision that involves receiving payments, the relevant requirements of PCI DSS must be considered. Apparent efficiencies and savings from new card processing methods may be at risk due to the time and cost of adhering to a more onerous PCI DSS compliance requirement.	

Appendix 3

Summary of Key Issues from audits previously reported to Committee

System/Area	Opinion	Area Reviewed	Date Issued	Comments	Management Actions Agreed & Follow-Up
Data Protection and security	Limited Assurance	Information is one of the most valuable assets held by any organisation. The council holds and processes large amounts of personal and sensitive data. Senior management recognise there are information governance risks associated with holding this information, and that appropriate practices need to be followed by staff. We performed an unannounced visit and review of Ryedale House in August 2015. The objective of the visit was to assess the extent to which data was being held securely in the council's offices. This included hard copy personal and sensitive information as well as electronic items such as laptops and removable media.	October 2015	**Strengths** The Council had addressed the findings from the 2013 audit with training and measures to improve staff awareness. Council procedures had also been updated. There is now increased awareness of the importance of securing personal and sensitive data. **Areas for improvement** We noted a number of instances where documents had not been secured. Council policies were not always being complied with, including the need for clear desks. In some instances lockable storage was not available. There is still a need to fully embed good information security practice at Ryedale House.	Management is taking a number of actions. In the short term the need for all sensitive information to be secured is to be clearly communicated to all staff. Lockable storage where needed will be provided. Management is also considering how best to manage overall data security on an ongoing basis. Areas such as policy, procedures and ongoing compliance training will form part of that work.
Server Rooms security	Limited Assurance	It is important to protect servers and other network infrastructure from fire, flood, power outages and other environmental hazards, and also potential damage, theft or sabotage. Weak physical security arrangements could also lead to unauthorised access to sensitive information. We reviewed the server room at Ryedale House and the Malton depot.	January 2016	**Areas for improvement** The council's servers at Ryedale House and the Malton depot are exposed to the risks of unauthorised access and potential disruption to, or loss of, data, services or operational activities due to important controls not being in place.	Management are currently considering the strategic and operational matters in respect of the management of the Server Rooms.

Appendix 4

Audit Opinions and Priorities for Actions

Audit Opinions	
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. Our overall audit opinion is based on 5 grades of opinion, as set out below.	
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 (was Moderate) 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.

Appendix 5

INTERNAL AUDIT QUALITY ASSURANCE AND IMPROVEMENT PROGRAMME

1.0 Background

Ongoing quality assurance arrangements

Veritau maintains appropriate ongoing quality assurance arrangements designed to ensure that internal audit work is undertaken in accordance with relevant professional standards (specifically the Public Sector Internal Audit Standards). These arrangements include:

- the maintenance of a detailed audit procedures manual
- detailed job descriptions and competency profiles for each internal audit post
- regular performance appraisals
- regular 1:2:1 meetings to monitor progress with audit engagements
- training plans and associated training activities
- the maintenance of training records and training evaluation procedures
- agreement of the objectives, scope and expected timescales for each audit engagement with the client before detailed work commences (audit specification)
- the results of all audit testing work documented using the company's automated working paper system (Galileo)
- file review by an audit manager and sign-off of each stage of the audit process
- post audit questionnaires (customer satisfaction surveys) issued following each audit engagement
- performance against agreed quality targets reported to each client on a regular basis.

On an ongoing basis, a sample of completed audit files is also subject to internal peer review by a senior audit manager to confirm quality standards are being maintained. The results of this peer review are documented and any key learning points shared with the internal auditors (and the relevant audit manager) concerned.

The Head of Internal Audit will also be informed of any general areas requiring improvement. Appropriate mitigating action will be taken (for example, increased supervision of individual internal auditors or further training).

Annual self-assessment

On an annual basis, the Head of Internal Audit will seek feedback from each client on the quality of the overall internal audit service. The Head of Internal Audit will also update the PSIAS self assessment checklist and obtain evidence to demonstrate conformance with the standards. As part of the annual appraisal process, each internal auditor is also required to assess their current skills and knowledge against the competency profile relevant for their role. Where necessary, further training or support will be provided to address any development needs.

The Head of Internal Audit is also a member of various professional networks and obtains information on operating arrangements and relevant best practice from other similar audit providers for comparison purposes.

The results of the annual client survey, PSIAS self-assessment and professional networking are used to identify any areas requiring further development and/or improvement. Any specific changes or improvements are included in the annual Improvement Action Plan. Specific actions may also be included in the Veritau business plan and/or individual personal development action plans. The outcomes from this exercise, including details of the Improvement Action Plan are also reported to each client. The results will also be used to evaluate overall conformance with the PSIAS, the results of which are reported to senior management and the board[3] as part of the annual report of the Head of Internal Audit.

External assessment

At least once every five years, arrangements must be made to subject internal audit working practices to external assessment to ensure the continued application of professional standards. The assessment should conducted by an independent and suitably qualified person or organisation and the results reported to the Head of Internal Audit. The outcome of the external assessment also forms part of the overall reporting process to each client (as set out above). Any specific areas identified as requiring further development and/or improvement will be included in the annual Improvement Action Plan for that year.

2.0 Customer Satisfaction Survey – 2016

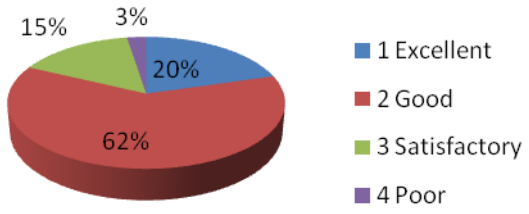
Feedback on the overall quality of the internal audit service provided to each client was obtained in May 2016. Where relevant, the survey also asked questions about the counter fraud and information governance services provided by Veritau. A total of 124 surveys (2015 – 103) were issued to senior managers in client organisations. 41 surveys were returned representing a response rate of 33% (2015 - 32%). The surveys were sent using Survey Monkey so the responses were anonymous. Respondents were asked to rate the different elements of the audit process, as follows:

- Excellent (1)
- Good (2)
- Satisfactory (3)
- Poor (4)

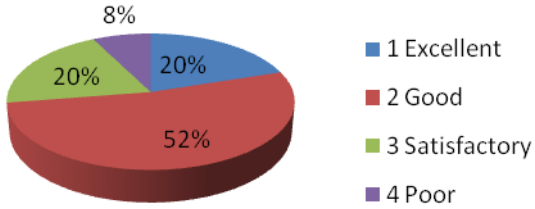
Respondents were also asked to provide an overall rating for the service. The results of the survey are set out in the charts below:

[3] As defined by the relevant audit charter.

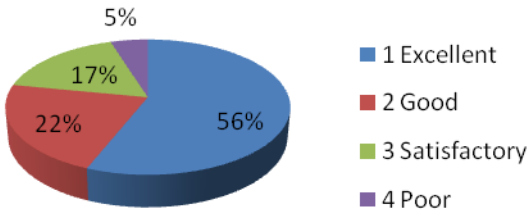
1 The quality of planning and the overall coverage of the audit plan



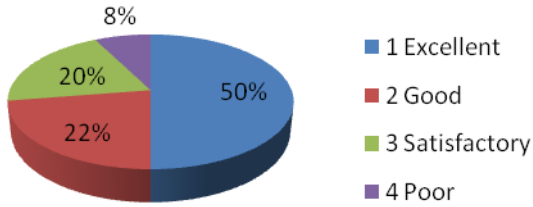
2 The provision of advice and guidance



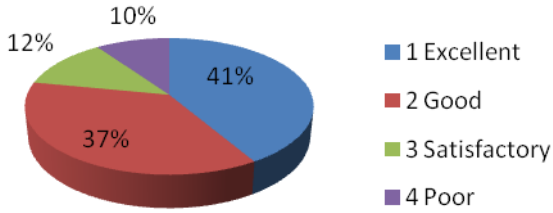
3 The conduct and professionalism of audit staff



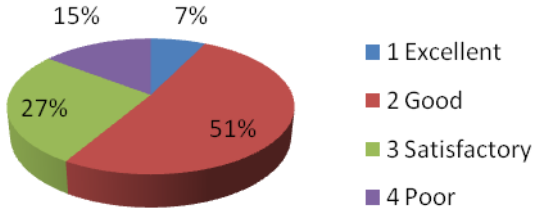
4 The ability of audit staff to provide unbiased and objective opinions



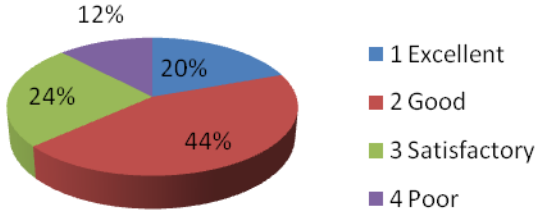
5 The ability of audit staff to establish a positive rapport with customers



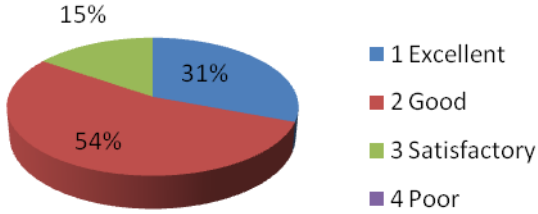
6 The auditors' overall knowledge of the system / service being audited



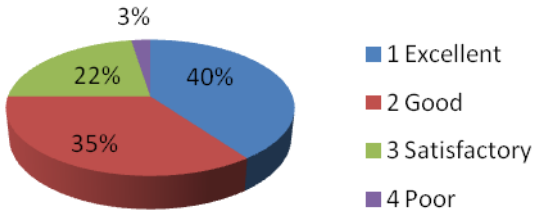
7 The auditors' ability to focus on the areas of greatest risk



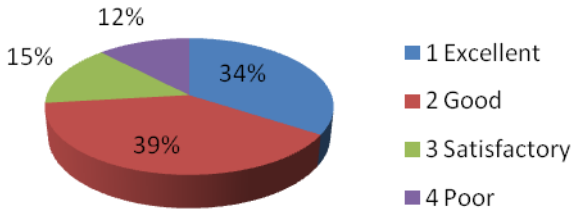
8 Agreeing the scope and objectives of the audit



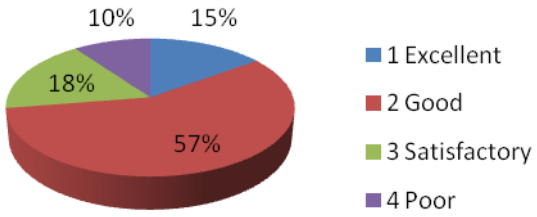
9 The auditors' ability to minimise disruption to the service being audited



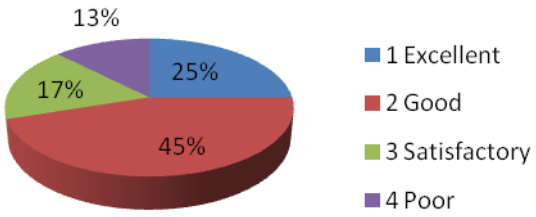
10 The communication of issues found by the auditors during their work



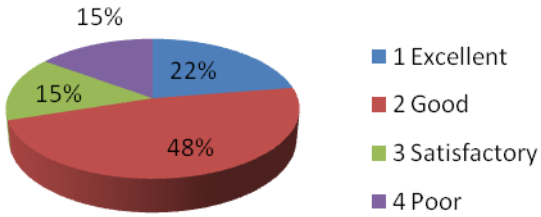
11 The quality of feedback at the end of the audit



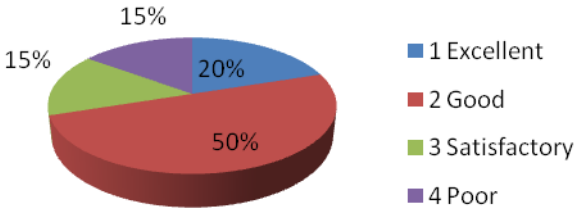
12 The accuracy, format, length and style of audit reports



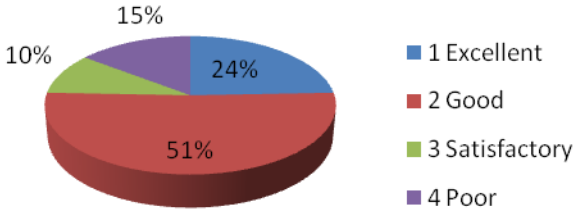
13 The relevance of audit opinions and conclusions



14 The extent to which agreed actions are constructive and practical



Overall rating for the Internal Audit services provided by Veritau



The overall ratings in 2015 were:

Excellent – 8 (27%)

Good – 19 (63%)

Satisfactory – 3 (10%)

Poor – 0 (0%)

The feedback shows that the majority of clients continue to value the service being delivered. A small number of respondents ranked the service as poor but did not provide any further comments or suggestions for improvement.

3.0 Self Assessment Checklist – 2016

The checklist prepared by CIPFA to enable conformance with the PSIAS and the Local Government Application Note to be assessed was originally completed in March 2014. Documentary evidence was provided where current working practices were considered to fully or partially conform to the standards.

In most areas the current working practices were considered to be at standard. However, a few areas of non-conformance were identified. None of the issues identified were however considered to be significant. In addition, in some cases, the existing arrangements were considered appropriate for the circumstances and hence required no further action.

The checklist has been reviewed and updated in 2016. The following areas of non-conformance remain unchanged:

Conformance with Standard	**Current Position**
Does the chief executive or equivalent undertake, countersign, contribute feedback to or review the performance appraisal of the Head of Internal Audit?	The Head of Internal Audit's performance appraisal is the responsibility of the board of directors. The results of the annual customer satisfaction survey exercise are however used to inform the appraisal.
Is feedback sought from the chair of the audit committee for the Head of Internal Audit's performance appraisal?	See above
Where there have been significant additional consulting services agreed during the year that were not already included in the audit plan, was approval sought from the audit committee before the engagement was accepted?	Consultancy services are usually commissioned by the relevant client officer (generally the s151 officer). The scope (and charging arrangements) for any specific engagement will be agreed by the Head of Internal Audit and the relevant client officer. Engagements will not be accepted if there is any actual or perceived conflict of interest, or which might otherwise be detrimental to the reputation of Veritau.

Conformance with Standard	Current Position
Does the risk-based plan set out the - (b) respective priorities of those pieces of audit work?	Audit plans detail the work to be carried out and the estimated time requirement. The relative priority of each assignment will be considered before any subsequent changes are made to plans. Any significant changes to the plan will need to be discussed and agreed with the respective client officers (and reported to the audit committee).
Are consulting engagements that have been accepted included in the risk-based plan?	Consulting engagements are commissioned and agreed separately.
Does the risk-based plan include the approach to using other sources of assurance and any work that may be required to place reliance upon those sources?	Whilst reliance may be placed on other sources of assurances there is no formal process to identify and assess such sources. However, assurance mapping will be used where appropriate and audit plans will highlight where other sources of assurance are being relied upon.

4.0 External Assessment

As noted above, the PSIAS require the Head of Internal Audit to arrange for an external assessment to be conducted at least once every five years to ensure the continued application of professional standards. The assessment is intended to provide an independent and objective opinion on the quality of internal audit practices.

Whilst the new Standards were only adopted in April 2013, the decision was taken to request an assessment at the earliest opportunity in order to provide assurance to our clients. The assessment was conducted by Gerry Cox and Ian Baker from the South West Audit Partnership (SWAP) in April 2014. Both Gerry and Ian are experienced internal audit professionals. The Partnership is a similar local authority controlled company providing internal audit services to over 12 local authorities (including county, unitary and district councils across Somerset, Wiltshire and Dorset).

The assessment consisted of a review of documentary evidence, including the self-assessment, and face to face interviews with a number of senior client officers and Veritau auditors. The assessors also interviewed an audit committee chair.

The conclusion from the external assessment was that working practices conform to the required professional standards. Copies of the detailed assessment report were provided to client organisations and, where appropriate, reported to the relevant audit committee.

5.0 Improvement Action Plan

Last year's quality assurance process identified the following required changes and improvements:

Change / improvement	Progress to date
The standard specification template will be updated to ensure that the expectations on Veritau and the relevant client organisation in terms of access to records and the distribution of reports (including the extent of any duty of care provided to third parties) are fully understood. Where appropriate, information sharing agreements will also be established with client organisations.	Completed. A new specification template has been adopted. Veritau has also signed the multi agency information sharing protocol. As well as its member councils, other signatories include North Yorkshire Police, North Yorkshire Fire and Rescue Authority plus various NHS organisations and housing associations.
Checklists will be provided to assist auditors ensure all stages of the audit process are fully completed on Galileo.	Completed.
Templates for 'non-standard' reports (for example – consultancy, fraud and special assignments) will be developed.	Completed.

The internal peer review has highlighted the need for further training to be provided on sampling and testing. This will be completed by 30 September 2016. No other changes or improvements to working practices have been identified as a result of this year's quality assurance process. To further enhance the overall effectiveness of the service, the Veritau business plan also includes a number of areas for further development, including:

- Preparation of a data analytics strategy
- Further development of in-house technical IT audit expertise
- Increased use of data matching to identify savings / data quality issues
- Development of a fraud awareness e-learning course.

6.0 Overall Conformance with PSIAS (Opinion of the Head of Internal Audit)

Based on the results of the quality assurance process I consider that the service generally conforms to the Public Sector Internal Audit Standards, including the *Definition of Internal Auditing*, the *Code of Ethics* and the *Standards*.

The guidance suggests a scale of three ratings, 'generally conforms, 'partially conforms' and 'does not conform'. 'Generally conforms' is the top rating and means that the internal audit service has a charter, policies and processes that are judged to be in conformance to the Standards. 'Partially conforms' means deficiencies in practice are noted that are judged to deviate from the Standards, but these deficiencies did not preclude the internal audit service from performing its responsibilities in an acceptable manner. 'Does not conform' means the deficiencies in practice are judged to be so significant as to seriously impair or preclude the internal audit service from performing adequately in all or in significant areas of its responsibilities.