Eastern Internal Audit Services

South Holland District Council

Progress Report on Internal Audit Activity

Period Covered: 4 January 2022 to 8 March 2022

Responsible Officer: Faye Haywood – Head of Internal Audit for South Holland District Council

CONTENTS

1. INTRODUCTION

1.1 This report is issued to assist the Authority in discharging its responsibilities in relation to the internal audit activity.

1.2 The Public Sector Internal Audit Standards also require the Chief Audit Executive to report to the Audit Committee on the performance of internal audit relative to its plan, including any significant risk exposures and control issues. The frequency of reporting and the specific content are for the Authority to determine.

1.3 To comply with the above this report includes:

- Any significant changes to the approved Audit Plan;
- Progress made in delivering the agreed audits for the year;
- Any significant outcomes arising from those audits; and
- Performance Indicator outcomes to date.

2. SIGNIFICANT CHANGES TO THE APPROVED INTERNAL AUDIT PLAN

2.1 The Annual Internal Audit Plan was approved on 29 July 2021. Since its approval the following audits have been proposed for deferral into future audit years.

Audit	Reason for deferral
SH2207 Legal Services	At the request of management, due to the service considering delivery options throughout the Partnership and no significant risks being raised, it is proposed this audit is deferred.
SH2204 Budget Sustainability Savings	This review has been postponed at the request of management to consider a co-ordinated approach across the Partnership.
SH2205 Digital Strategy	This review has been postponed at the request of management to consider a co-ordinated approach across the Partnership.

3. PROGRESS MADE IN DELIVERING THE AGREED AUDIT WORK

3.1 **Appendix 1** covers progress made against the 2021/22 internal audit plan. A total of 106 days of work has been completed equating to 63% of the overall agreed Internal Audit Plan.

Audit Lincolnshire's coverage includes the testing of key financial systems managed by Public Sector Partnership Services on behalf of South Holland District Council. The Head of Internal Audit places reliance on the work carried out by Audit Lincolnshire when concluding on the overall Internal Audit Opinion.

4. THE OUTCOMES ARISING FROM OUR WORK

4.1 On completion of each individual audit an assurance level is awarded using the following definitions:

Substantial Assurance: Based upon the issues identified there is a robust series of suitably designed internal controls in place upon which the organisation relies to manage the risks to the continuous and effective achievement of the objectives of the process, and which at the time of our review were being consistently applied.

Reasonable Assurance: Based upon the issues identified there is a series of internal controls in place, however these could be strengthened to facilitate the organisation's management of risks to the continuous and effective achievement of the objectives of the process. Improvements are required to enhance the controls to mitigate these risks.

Limited Assurance: Based upon the issues identified the controls in place are insufficient to ensure that the organisation can rely upon them to manage the risks to the continuous and effective achievement of the objectives of the process. Significant improvements are required to improve the adequacy and effectiveness of the controls to mitigate these risks.

No Assurance: Based upon the issues identified there is a fundamental breakdown or absence of core internal controls such that the organisation cannot rely upon them to manage risk to the continuous and effective achievement of the objectives of the process. Immediate action is required to improve the controls required to mitigate these risks.

4.2 Recommendations made on completion of audit work are prioritised using the following definitions:

Urgent (priority one): Fundamental control issue on which action to implement should be taken within 1 month.

Important (priority two): Control issue on which action to implement should be taken within 3 months.

Needs attention (priority three): Control issue on which action to implement should be taken within 6 months.

4.3 In addition, on completion of audit work "Operational Effectiveness Matters" are proposed, these set out matters identified during the assignment where there may be opportunities for service enhancements to be made to increase both the operational efficiency and enhance the delivery of value for money services. These are for management to consider and are not part of the follow up process.

4.4 During the period covered by the report Internal Audit has issued three reports in final as can be seen in the table below:

Audit	Assurance	P1	P2	P3
Cyber Security	Reasonable	0	3	8
Licensing	Substantial	0	0	2
Payroll (Audit Lincolnshire)	Reasonable	0	3	0

The Executive Summaries of these reports are attached at **Appendix 2**, full copies can be requested by Members.

4.5 As can be seen in the table above, as a result of these audits 16 recommendations have been raised and agreed by management.

4.6 During this period, a position statement for Corporate Fuel Cards has also been issued in final. The position statement has not resulted in any suggested actions/improvements for consideration. However, the auditor discussed suggestions with officers on the need to consider improved business intelligence over the use of fuel and bearer cards as part of the current procurement exercise, with the current contract due to expire on 31 March 2022.

5. PERFORMANCE MEASURES – Eastern Internal Audit Services

5.1 The Internal Audit Services contract includes a suite of key performance measures against which TIAA will be reviewed on a quarterly basis.

5.2 There are individual requirements for performance in relation to each measure; however, performance will be assessed on an overall basis as follows:

- 9-11 KPIs have met target = Green Status.
- 5-8 KPIs have met target = Amber Status.
- 4 or below have met target = Red Status.

Where performance is amber or red a Performance Improvement Plan will be developed by TIAA and agreed with the Internal Audit Consortium Manager to ensure that appropriate action is taken.

5.3 The contractor has concluded all allocated quarter two work and is making progress on outstanding quarter three and quarter four work. Delays have been experienced during the re-prioritisation of audit work with the available resources. No concerns are currently raised about the ability to conclude the annual internal audit opinion. This position is reviewed on a weekly basis with the contractor.

APPENDIX 1 – PROGRESS IN COMPLETING THE AGREED AUDIT WORK

Audit Area	Audit Ref	No. of days	Revised Days	Days Delivered	Status	Assurance Level	Recommendations				Date to Committee
							Urgent	Important	Needs Attention	Op	
Quarter 2											
COVID-19 Business Grants	SH2203	8	8	8	Final report issued 28 October 2021.	Substantial	0	0	2	0	November 2021
TOTAL		**8**	**8**	**8**							
Quarter 3											
Operational Fleet Review	SH2209	8	8	8	Position statement issued 4 January 2022.	Position Statement					March 2022
Corporate Health and Safety	SH2206	8	8	8	Draft report issued on 14 February 2022.						
Private Sector Housing DFGs	SH2211	12	12	9	Fieldwork complete. Draft report in preparation.						
TOTAL		**28**	**28**	**25**							
Quarter 4											
Performance Management, Corporate Policy and Business Planning	SH2201	10	10	7	Fieldwork complete. Draft report in preparation.						
Human Resources	SH2202	7	7	0	Scoping underway						
Budget Sustainability Savings	SH2204	10	0	0	Deferred to 2022-23.						
Digital Strategy	SH2205	10	0	0	Deferred to 2022-23.						
Legal Services	SH2207	10	0	0	Deferred to 2022-23.						
Licensing	SH2208	10	10	10	Final report issued on 3 March 2022.	Substantial	0	0	2	0	March 2022
Housing needs, allocation, homelessness, housing register	SH2210	10	10	5	Fieldwork underway.						
TOTAL		**67**	**37**	**22**							
IT Audits											
Cyber Security	SH2212	8	8	8	Final report issued 1 March 2022.	Reasonable	0	3	8	0	March 2022
Problem and Change Management	SH2213	8	8	5	Fieldwork complete. Draft report in preparation.						
TOTAL		**16**	**16**	**13**							
Follow Up											
Follow Up	N/A	10	10	8							
TOTAL		**10**	**10**	**8**							
TOTAL		**129**	**99**	**76**			**0**	**3**	**12**	**0**	
Percentage of TIAA plan completed				**77%**							
Audit delivered by Audit Lincolnshire											
Key Controls & Assurance	N/A	40	40		Due for end of quarter four						
Payroll	N/A	5	5	5	Final report issued 22 February 2022	Reasonable	0	3	0	0	Mar-22
Housing Benefit Subsidy	N/A	25	25	25	Report issued	Substantial	0	0	0	0	Nov-21
TOTAL		**70**	**70**	**30**			**0**	**3**	**0**	**0**	
				43%							
OVERALL TOTAL		**199**	**169**	**106**			**0**	**6**	**12**	**0**	
				63%							

APPENDIX 2 – AUDIT REPORT EXECUTIVE SUMMARIES

Maturity Assessment of Cyber Security

Executive Summary

OVERALL ASSURANCE ASSESSMENT

ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Engagement and Training	0	1	2	0
Architecture and Configuration	0	0	2	0
Logging and Monitoring	0	0	2	0
Supply Chain Security	0	2	2	0
Total	**0**	**3**	**8**	**0**

No recommendations were raised in the areas of Cyber Risk Management, Asset Management, Vulnerability Management, Identity and Access Management, Data Security and Incident Management

SCOPE

This maturity assessment has focussed on the National Cyber Security Centre's revised 10 steps to Cyber Security framework that covers Cyber Risk Management, Engagement and Training, Asset Management, Architecture and Configuration, Vulnerability Management, Identity and Access Management, Data Security, Logging and Monitoring, Incident Management and Supply Chain Security.

Introduction

1. Organisations are facing an increasing risk of Cyber incidents and Cyber-crime. A key step to reducing the risk and protecting organisations in this area is understanding the maturity of your organisation in terms of how Cyber risks are managed. The data within this report is derived from supporting management with a self-assessment of their maturity in the following 10 recognised areas of Cyber Security:

• Cyber Risk Management	• Identity and Access Management
• Engagement and Training	• Data Security
• Asset Management	• Logging and Monitoring
• Architecture and Configuration	• Incident Management
• Vulnerability Management	• Supply Chain Security

2. The Cyber Security world is in need of a mature approach to managing cyber risk, because attackers continue to develop new threats beyond current knowledge. The fact that emerging threats are increasing is driving organisations to adopt a predictive attitude to address these threats. In order to protect themselves all organisations information assets and ICT systems need to be secured, managed and monitored.

3. Levels of recorded Cybercrime continue to grow. The Telephone-operated Crime Survey for England and Wales (TCSEW) showed that there were 1.9 million computer misuse offences in the year ending September 2021. This was an 89% increase compared with the year ending September 2019, largely driven by a 161% increase in “Unauthorised access to personal information (including hacking)” offences. This reinforces the need for users to implement robust e-Safety, including passwords based on “Three things” and not re-using the same password within multiple IT systems or websites. The National Cyber Security Centre (NCSC) provides guidance for sectors, and for users to help address the gap between good security and dangerous practices.

4. The Covid-19 Pandemic has also been instrumental in increasing risks associated with Cyber Crime. Many attacks are thematic in nature and continue to exploit users’ interest in the latest pandemic news including around access to vaccinations. Coupled with a rapid IT transformation to enable home working with new IT systems and products, the associated likelihood of cybercrimes manifesting has also increased.

5. The potential impact from cybercrime can be of substantial damage to the operational capability of the organisation. Legislative impact is within the scope of the Data Protection Act 2018, which embodies the General Data Protection Regulations (GDPR). It requires data to be processed in a manner that ensures its security. This includes protection against unauthorised or unlawful processing, accidental loss, destruction or damage. This places a requirement on all organisations to ensure that appropriate technical and organisational measures are in place. The potential level of fines for Data Protection breaches (including as a result of hacking) are up to 20m Euros / £18m or 4% of global annual turnover whichever is the greater. In addition to the financial penalties, breaches cause significant reputational damage to affected organisations, including those using cloud based IT services.

6. In assessing maturity, the current maturity level for each of the 10 areas has been identified and management's aspirations and appetite for improvement to manage and mitigate risk have been ascertained. This work was carried out between December 2021 and February 2022 by the Cyber Assurance team as part of the proactive Internal Audit programme for 2021/22.

7. TIAA's Cyber Maturity model is based on the traditional maturity model, and comprises of levels 0-5 as described below:

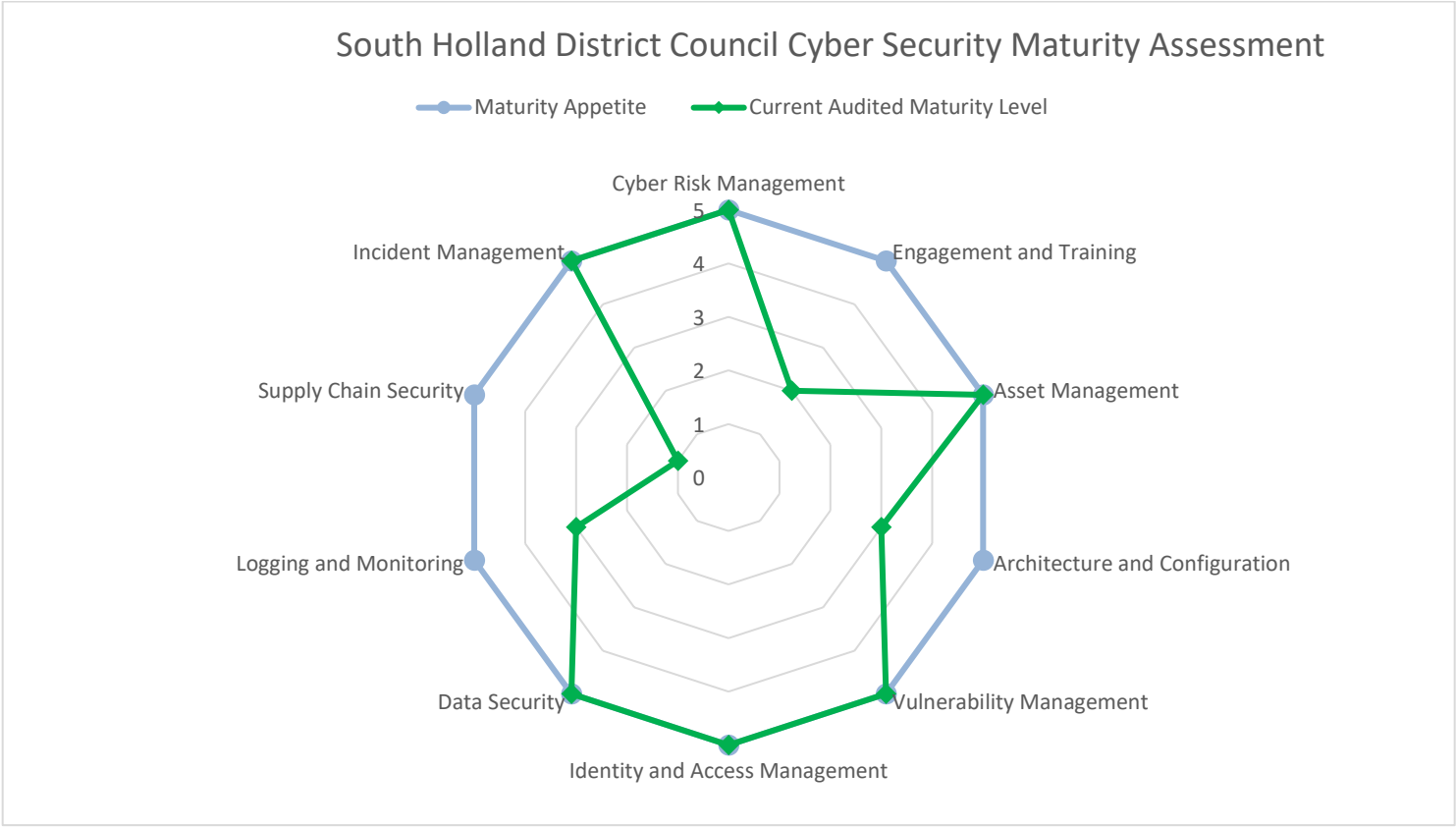
Level	Status	Description
0	Incomplete	The process is not implemented or fails to achieve its process purpose. At this level, there is little or no evidence of any systematic achievement of the process purpose.
1	Initial	Unpredictable process that is poorly controlled and reactive
2	Managed	Process is planned, documented and monitored ad-hoc and is often reactive
3	Defined	Proactive process meant for organizations
4	Quantitative	Measured and controlled process
5	Optimising	Focus is on continuous process and improvement

Summary

8. The review noted that management rated South Holland District Council's dependency on Information technology as High and recognised that Cyber-crime was a significant risk. Management considered that untreated cyber risks were at a Medium level. It was noted that the organisation has invested in improving cyber security measures in the last 12 months.

9. The Council has not experienced any significant cyber incidents within the last 12 months. However, there are processes in place that monitor and detect potential incidents, allowing for relevant triage and resolution to take place in a timely manner. An example of this is the recent Log4J Malware. This incident had a Low impact on the Council, and recovery was achieved within four days without impact on the Council's business.

10. TIAA's maturity assessment is summarised in the radar diagram below. Significant gaps or two or more maturity steps exist between the aspirational level of maturity and the assessed level for the following process areas: Engagement and Training, Architecture and Configuration, Logging and Monitoring and Supply Chain Security.



11. Where gaps have been identified management should consider TIAA's maturity improvement recommendations within this report (summarised at Appendix A) to further control and mitigate cyber risks.

Rec.	Cyber Area	Finding	Recommendation	To Achieve Maturity Level
ET 3	Engagement and Training (Important)	Level 3 maturity is not fully achieved.	The organisation must provide annual, structured cyber and information security training under an appropriate training programme to all staff. We have noted that take up of training has been weak at the Council but that there has been very recent senior leadership resolutions to reinforce the need to implement and complete appropriate, regular Cyber training programmes.	3
ET 4	Engagement and Training (Needs Attention)	Level 4 maturity is not fully achieved.	Awareness programmes and materials to be provided to staff on a proactive basis, not just in reaction to incidents and events. Our testing of this requirement noted that it may have been able to be marked as compliant in its own right. However, full compliance is reliant on previous levels also being fully compliant.	4
ET 5	Engagement and Training (Needs Attention)	Level 5 maturity is not fully achieved.	Training content must be refreshed periodically to ensure that content is relevant and covers current risks and threats. We have noted that, historically, there has been some work by PSPSL to help comply with this requirement – the document known as “Current and Future Training Proposal”. However, available evidence suggests that the work requires review as it is older and no longer relevant to current needs.	5
AC 4	Architecture and Configuration (Needs Attention)	Level 4 maturity is not fully achieved.	Anti-malware defences must be deployed for all server and endpoint systems. Anti-malware solutions must be up to date and its capability commensurate with the malware threat to the organisation. Our audit testing suggests that these processes are in place but that monitoring and remediation of any errors found is weak.	4
AC 5	Architecture and Configuration (Needs Attention)	Level 5 maturity is not fully achieved.	External assurances must be sought on the security of the organisation’s digital architecture and configurations. Our audit testing suggests that this level would have been compliant in its own right. However, it can only be marked as Partial compliance due to the weakness noted at level Four.	5
LM 4	Logging and Monitoring (Needs Attention)	Level 4 maturity is not fully achieved.	Log and monitoring analysis for incidents must take place, with identified issues escalated to technical staff. We have noted that there is further work required to complete the integration of NXLogs into the wider monitoring process.	4

Rec.	Cyber Area	Finding	Recommendation	To Achieve Maturity Level
LM 5	Logging and Monitoring (Needs Attention)	Level 5 maturity is not fully achieved.	Monitoring effectiveness must be reviewed on a regular basis to determine adequacy of monitoring controls. We have noted that there is work to improve compliance at level Four, which, by definition, means that level Five is fully compliant in its own right. However, a Partial compliance is being assigned due to the fact that level Four is also Partial.	5
SCS 2	Supply Chain Security (Important)	Level 2 maturity is not fully achieved.	The cyber security supply chain must be fully documented and current controls mapped out.	2
SCS 3	Supply Chain Security (Important)	Level 3 maturity is not fully achieved.	Third-party IT contracts must include incident response requirements of the organisation in the event of an incident.	3
SCS 4	Supply Chain Security (Needs Attention)	Level 4 maturity is not fully achieved.	Regular assurance must be obtained from third-parties to provide confidence in supplier's security measures and controls.	4
SCS 5	Supply Chain Security (Needs Attention)	Level 5 maturity is not fully achieved.	IT suppliers must be reviewed periodically to ensure that they are meeting contractual security obligations and key performance targets.	5

Assurance Review of the SH2208 Licencing

Executive Summary

OVERALL ASSURANCE ASSESSMENT

ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Policies and Procedures	0	0	1	0
Complaints, appeals and revocations of licenses	0	0	1	0
Total	**0**	**0**	**2**	**0**

No recommendations have been raised in respect of processing applications (new and renewals) including panel hearings and committee process registrations, and recording and reconciliation of income (including fees).

SCOPE

The objective of the audit was to review the systems and controls in place within Licensing, to help confirm that these are operating adequately, effectively and efficiently. The audit covered policies and procedures; processing applications (new and renewals) including panel hearings and committee process registrations; complaints, appeals and revocations of licenses; and recording and reconciliation of income (including fees).

RATIONALE

- The systems and processes of internal control are, overall, deemed 'Substantial Assurance' in managing the risks associated with the audit. The assurance opinion has been derived as a result of two 'needs attention' recommendations being raised upon the conclusion of our work.
- Licencing was last reviewed in 2016/17 (jointly with Breckland) and given a reasonable assurance grading. The review focused on licensing of Hackney Carriage and Private Hire Vehicles and Operators and receipting of income.

POSITIVE FINDINGS

It is acknowledged there are areas where sound controls are in place and operating consistently:

- The Council has an up to date Gambling Act 2005 policy dated January 2022 which adhered to guidance issued by the Gambling Commission. The policy provides clarity to applicants, interested parties and responsible authorities on how Council will determine applications.
- The Council's website has details on how to apply for the different licences issued by the Council to ensure the general public have access to the information.
- The Council has an up to date Statement of Licensing Policy dated 2021-2026 which makes reference to the Licensing Act (2003). The policy ensures the promotion of the licensing objectives through the effective regulation of licensed premises, qualifying clubs and temporary events.
- New licences and renewal licences are issued by the Council in accordance with relevant policies and procedures to ensure public safety.
- Revocation of licences and application for variation of licences are considered by the Panel of the Committee of the Licensing Authority or the Licensing Panel in accordance with their delegated authority to ensure public safety.
- The Council receives correct fees prior to issuing of licences to ensure relevant fund due to the Council are collected and accounted for.
- Payment for licences is made through the Capita payment system (Capita) with a notification email sent via Capita to the Licencing Team. The payment confirmation received is used to update the individual applicant account on Tascomi.
- Quarterly meetings are held between the Service Accountant and the Head of Public Protection to ensure that the licencing team financial performance is monitored regularly.

ISSUES TO BE ADDRESSED

The audit has highlighted the following areas where two 'needs attention' recommendations have been made.

Policies and Procedures

- Hackney Carriage and Private Hire Licensing Procedures Policy dated May 2014 be updated, thereby ensuring they are reflective of current standards.

Complaints, Appeals and Revocations of licenses

- Complainant be notified of the outcome of their complaints in a timely manner to ensure the Council continue to receive notifications from the public in respect of people carrying out licensing activities without the right licences.

Operational Effectiveness Matters

There are no operational effectiveness matters for management to consider.

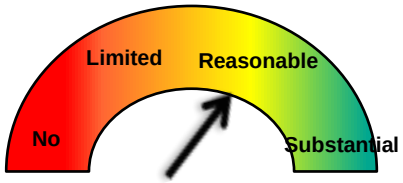
Previous audit recommendations

The audit reviewed the previous internal audit recommendations, of which two remain outstanding relating to updating of the Hackney Carriage and Private Hire Licensing Policy and having a documented procedures for complaint handling. These were discussed with management have been superseded by the recommendations raised within this audit.

Other Issues Noted

- The decision to stop routine inspections due to the national lockdown and risk of Covid-19 was taken through the Council's Gold command structure and approved by the Council Leader under delegated authority. Review of the Management Team meeting notes dated 6th August 2020 confirmed that Public Protection (includes licensing) can now resume inspections if needed using the 'Covid 19 Guidance- Carry Out Essential Visits' and the 'Generic COVID 19 Risk Assessment/Action Plan Visits/Inspection'.
- Digital licence applications are now received by the Licencing Team via email and processed in the same way as hard copy applications.
- South Holland District Council and Breckland Councils have started the process of separating the public protection data on Tascomi to two separate systems. The scoping meeting was held with IDOX in February 2022 to discuss how the project will be carried out.

Payroll Audit – Executive Summary



Reasonable Assurance

Our critical review or assessment on the activity gives us a reasonable level of confidence on service delivery arrangements, management of risks, and operation of controls and / or performance.

There are some improvements needed in the application of controls to manage risks. However, the controls have been evaluated as adequate, appropriate, and operating sufficiently so that the risk of the activity not achieving its objectives is medium to low

Risk	Rating (R-A-G)	Recommendations	
		High	Medium
Systems access is not restricted, payments are fraudulent or incorrect	Medium	0	1
Payments are fraudulent or incorrect	Medium	0	1
Payment runs have not actually been processed/processing is incomplete or are incorrect	Medium	0	1
Exception reporting to detect payroll errors is not effective	Low	0	0
Third party payments/deductions and information are not provided to statutory agencies as required	Low	0	0
TOTAL		0	3

Key Messages

We included a review of the impact of the implementation of the new payroll system to ensure that there are adequate key controls in place to mitigate the risk of fraud and error within this system. We found areas of good practice with some controls operating effectively in the new system. We also found key areas where controls seemed less effective but there are compensating checks in place where necessary.

There is an ongoing project to work with the provider to manage remaining system development issues and workarounds, this is being lead by Payroll and Reward Manager with oversite from HR Project Manager.

Our review has provided **Reasonable assurance**.

Our opinion is based on testing and discussions with the Payroll team. At the time of the audit we did not find any significant errors in the payroll payments although we found the following issues –

- At the time of audit the three payroll officers had super user access to the Payroll and HR system, similar to the arrangement for the previous payroll system. Whilst this could be seen as increasing the risk of fraud, there are a number of reports and checks used to overcome any potential misuse.
- The current controls include the payroll manager carrying out independent checks and reviews along with finance being provided with reports for liaison with budget managers. However there is no formal acknowledgement that this has taken place and assumes that all is correct unless advised.
- We found one error in payroll that impacted on an employees pay, which had not been detected and corrected by the Payroll monitoring systems but was corrected the following month.
- As with many payroll systems, there are a number of manual interventions required to process an accurate payroll. Where possible these should be reviewed with the provider to become automatic. Manual processes increase resource requirements and the risk of error or fraud.
- There is a snag list of actions still to be implemented by the providers of the new system. Review of this showed that some actions were incomplete and had passed their deadline date for resolution.
- At the time of the audit review the Council (client) was receiving verbal updates on the progress and delivery of the new system. More robust evidence based assurance should be sought to provide certainty on delivery and issues solution.

Because of the issues highlighted above our opinion is that at the present time we can give **Reasonable** assurance around the payroll function.

Post audit update

Since carrying out the review we have been advised and assurred that the access levels have now been revised to ensure appropriate segregation between HR and Payroll officers.

In addition the budget holders and business partners are being reminded of their responibilities in checking and verifying the payroll reports and returns.
These amendments, do not affecting our assurance rating as the other concerns remain at this time.

Areas of Good Practice

During our review we found that:-

- Check lists are in place to ensure all essential actions are completed for the accuracy of payroll administration.
- Third party payments reviewed had been authorised appropriately in line with Council's Financial procedure rules and had been processsed accurately and timely.
- Net pay is approved in line with Council's financial procedures.
- Claims are processed through workflow systems ensuring relevant authorisation and supporting documentation.
- Robust closedown process in place which checks balances and pay variance reports to ensure any fundemental errors would be identified.
- Contracts were issued prior to commencement of employment.
- September KPI for Payroll reported a 99.54% accuracy rating.

Management Response

PSPS would like to take this oppertunity to thank Assurance Lincolnshire for the time in undertaking this Payroll Key Controls Audit; it is pleasing to see that there are a number of key areas with good practice and that overall PSPS has good risk management in place.

The audit was undertaken following the implementiation of a new HR and Payrol system, as such every month PSPS has been working to improve and streamline our processes to ensure continuious imporvement.

PSPS are particually proud to be able to report consistently above 99.5% payroll accuracy particually whilst implementing a new system.

This report highlights several recommendations which I am pleased to say the majority have already been compelted, details of this can be found within the agreed action plan.

Nikki Harding
Head of HR & OD
19th Janaury 2022