Eastern Internal Audit Services

South Holland District Council

Progress Report on Internal Audit Activity

Period Covered: 1 October 2018 to 7 January 2019

Responsible Officer: Emma Hodds – Head of Internal Audit for South Holland District Council

Faye Haywood – Internal Audit Manager 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   At the meeting on 15 March 2018, the Annual Internal Audit Plan for the year was approved, identifying the specific audits to be delivered. Since then, the following changes to the plan have been made;

Audit description	Nature of the change
Transformation Programme	The programme has come to natural end of the four-year life span, the remaining efficiencies are part of the ongoing programme of work, therefore the internal audit is no longer required.
CBPS – Finance	Two days from the transformation programme budget have been utilised within this audit to ensure that a robust review of budget setting can be undertaken to fully review the risks.
Environmental Protection	This audit has been deferred to 2019/20 to allow the team to work on the implementation of new software.
Office 365 changed to Service Desk	The Office 365 project has not progressed as far as the team anticipated at the time of audit planning. However, this is a massive project for the Council and it was agreed that some audit oversight is needed, as the project will be regularly reviewed through the IT and Comms Board it was agreed that the agenda, reports and minutes from these discussions would be shared with Internal Audit so that a consultancy role can be undertaken. A review of the Service Desk has been brought forward for internal audit review.

3.   PROGRESS MADE IN DELIVERING THE AGREED AUDIT WORK

3.1   The current position in completing audits to date within the financial year is shown in **Appendix 1** and progress to date is in line with expectations.

3.2   In summary 143 days of programmed work has been completed, equating to 57% of the (revised) Audit Plan for 2018/19.

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 Services has issued four final reports:

Audit	Assurance	P1	P2	P3
Food, Health and Safety (*)	Reasonable	0	2	2
Democratic Services (*)	Reasonable	0	4	3
Cyber Security	Reasonable	0	5	0
Software Licencing	Reasonable	0	1	0

The Executive Summary of this report is attached at **Appendix 2**, a full copy of this report can be requested by Members. (*) these audit reviews were carried out jointly and the table reflects the recommendations that relate to South Holland only.

4.5   As can be seen in the table above as a result of these reports 17 recommendations have been raised.

4.6.1   All recommendations have been agreed by management. In addition, four Operational Effectiveness Matters have been proposed to management for consideration.

4.7   It is pleasing to note that these audits have concluded in a positive opinion being awarded, indicating a strong and stable control environment to date, with no issues that would need to be considered at year end and included in the Annual Governance Statement.

5.   PERFORMANCE MEASURES

5.1   The Internal Audit Services contract includes a suite of key performance measures against which the contractor will be reviewed on a quarterly basis, there are a total of 11 indicators, over four areas.

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 the contractor and agreed with the Internal Audit Manager to ensure that appropriate action is taken.

5.3   The first quarters work has been completed, with quarter two and quarter three near to finalisation. A report on the performance measures is provided to the Internal Audit Manager and progress is being closely monitored with the contractor to ensure work is progressed to ensure a year end opinion can be provided.

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 1											
Environmental Services including waste, recycling & depot services	SH1902	16	16	16	Final report issued 13 September 2018	Reasonable	0	1	4	1	October 2018
TOTAL		**16**	**16**	**16**							
Quarter 2											
Procurement & Contract Management	SH1901	8	8	7	Draft report issued						
Compass Point - Finance	SH1903	10	12	8	Audit underway						
Food, Health & Safety	SH1905	8	8	8	Final report issued 4 October 2018	Reasonable	0	2	2	0	January 2019
Democratic Services	SH1906	8	8	8	Final report issued 21 November 2018	Reasonable	0	4	3	2	January 2019
TOTAL		**34**	**36**	**31**							
Quarter 3											
Corporate Governance	SH1908	4	4	3	Draft report issued						
Payroll and Human Resources	SH1909	15	15	7	Audit underway. Draft report by January						
Delivery Unit Team	SH1910	6	6	3	Audit underway. Draft report by January						
Leisure	SH1911	10	10	5	Audit underway. Draft report by January						
Community Safety & ASB	SH1907	12	12	6	Audit underway. Draft report by January						
Building Control	SH1912	8	8	7	Draft report issued						
TOTAL		**55**	**55**	**31**							
Quarter 4											
Asset Management	SH1904	10	10	0							
Transformation Programme	SH1913	6	0	0	Cancelled						
Environmental Protection	SH1914	8	0	0	Audit deferred until 2019/20						
Housing Needs, Allocations, Homelessness and Housing Register	SH1915	30	12	1	APM issued Audit start January 2019						
Housing - Property Services	SH1920	0	18	0							
TOTAL		**54**	**40**	**1**							

Audit Area	Audit Ref	No. of days	Revised Days	Days Delivered	Status	Assurance Level	Recommendations				Date to Committee
							Urgent	Important	Needs Attention	Op	
IT Audits											
Office 365 Service Desk	SH1916	5	6	0							
Cyber Security	SH1917	10	10	10	Final report issued 22 November 2018	Reasonable	0	5	0	0	January 2019
Network Management	SH1918	5	5	0							
Software Licensing	SH1919	5	5	5	Final report issued 10 December 2018	Reasonable	0	1	0	2	January 2019
TOTAL		**25**	**26**	**15**							
Follow Up											
Follow Up	NA	12	12	9							
TOTAL		**12**	**12**	**9**							
TOTAL		**196**	**185**	**103**			0	13	9	5	
Percentage of plan completed				**56%**							
Audit delivered by East Lindsey District Council											
Key Controls & Assurance	tbc	40									
Revenues			6	3	Terms of Reference, report due January 2019						
Benefits			6	3	Terms of Reference issued, report due January 2019						
(Payroll)											
Housing Rents			5	3	Terms of Reference issued, report November 2018. Currently delayed.						
Financial Services: Accounts Receivable Accounts Payable Budget Management Income Asset Management			15	2	Terms of Reference issued, report due March 2019						
Accountancy Services (general ledger, control accounts, treasury management & bank reconciliation)			6	3	Terms of Reference issued, report due January 2019						
Housing Benefit Subsidy	tbc	25	25	25							
Follow Up			2	1							
		65	**65**	**40**							
				62%							
OVERALL TOTAL		**261**	**250**	**143**							
				57%							

Assurance Review of Food, Health and Safety

Executive Summary

OVERALL ASSURANCE ASSESSMENT

ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Policies and procedures	0	0	1	0
Food safety – registration	0	1	0	0
Food safety – hygiene inspections	0	1	0	0
Food safety – complaints	0	0	1	0
Total	**0**	**2**	**2**	**0**

No recommendations have been raised in respect of infectious diseases or health and safety.

SCOPE

The objective of the audit was to review the adequacy, effectiveness and efficiency of the systems and controls in place over Food, Health and Safety.

RATIONALE

- The systems and processes of internal control are, overall, deemed 'Reasonable' in managing the risks associated with the audit. The assurance opinion has been derived as a result of two 'important' and two 'needs attention' recommendations being raised upon the conclusion of our work.

- The areas under scope have not been subject to previous audit scrutiny by TIAA at either authority, hence no direction of travel is provided with the overall assurance opinion.

POSITIVE FINDINGS

We found that the Council has demonstrated the following points of good practice as identified in this review and we will be sharing details of these operational provisions with other member authorities in the Consortium:

- South Holland District Council has taken over the lead from Boston Borough Council in developing the local Safety Advisory Group, which is a network of various organisations including Lincolnshire County Council, police, fire and ambulance services, with the purpose being to consult and advise on safety issues relating to major events taking place in the district. As a result of the changes made, the number of meetings has been significantly reduced to ensure that the group is organised efficiently and to reduce time commitments for all parties involved.

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

- The Councils use alternative inspection questionnaires for low risk premises to reduce the number of inspections required, thereby maximising officer time on higher risk cases.

- South Holland District Council works closely with the Fresh Produce Consortium (FPC), which represents businesses, in developing a process for responding to incidents of clandestine travellers in shipments of food. This allows for a consistent response which is acceptable to all parties and provides the Council with greater confidence in the controls in place and in the businesses dealing with these incidents.

- Proactive health and safety work is conducted via projects looking at identified high risk areas, to ensure that the greatest risks are still addressed.

ISSUES TO BE ADDRESSED

The audit has also highlighted the following areas where two 'important' recommendations have been made.

Food hygiene – registration

- Checks are made for all new food business registrations to ensure that the business owner has not been prohibited from operating a food business. This will reduce the risk of such persons operating a food business in the district, thereby posing a health risk to the public. (South Holland)

Food hygiene – inspections

- All food hygiene inspections, including initial inspections of new businesses and routine inspections, and responses to complaints are conducted in accordance with target timescales, to reduce the risk of poor food hygiene practices being followed and consequent reputational damage to the Councils. (Both Councils)

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

Policies and procedures

- Procedures and work instructions are reviewed and updated as required, to reduce the risk of outdated working practices being followed. (Both Councils)

Food hygiene – complaints

- All evidence relating to food complaint cases and publicly funded funerals to be retained electronically and linked to a central database, to reduce the risk of it being unavailable when required. (South Holland)

Operational Effectiveness Matters

There are no operational effectiveness matters for management to consider.

Previous audit recommendations

The areas under scope have not been subject to previous audit scrutiny by TIAA at either authority.

Other issues noted

During the audit it was noted that the approved version of the Councils' joint Corporate Enforcement Policy was not available on the South Holland District Council website. This issue was addressed during the audit and therefore a recommendation has not been raised.

Assurance Review of Democratic Services Arrangements

Executive Summary

OVERALL ASSURANCE ASSESSMENT

REASONABLE ASSURANCE

- SUBSTANTIAL ASSURANCE
- REASONABLE ASSURANCE
- LIMITED ASSURANCE
- NO ASSURANCE

ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Training	0	3	1	1
Members' Allowances	0	0	1	1
Members' Expenses	0	3	3	0
Total	**0**	**4**	**3**	**2**

SCOPE

The objective of the audit was to review the adequacy, effectiveness and efficiency of the systems and controls in place over Democratic Services.

RATIONALE

- The systems and processes of internal control are, overall, deemed "Reasonable" in managing the risks associated with the audit. The assurance opinion has been derived as a result of six 'important' and five 'needs attention' recommendations being raised upon the conclusion of our work.

- The audit has also raised two 'operational effectiveness matters', which sets 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.

- A review of Democratic Services (BRK/16/06) was completed as part of the 2015/16 audit plan for Breckland DC, with the final report being issued in October 2015. The audit concluded in a 'Substantial' assurance opinion, with no recommendations being raised. Hence there has been a deterioration since the previous review.

- This area has not been subject to previous audit scrutiny at South Holland by TIAA. As such, no direction of travel is applicable.

POSITIVE FINDINGS

We found that the Council has demonstrated the following points of good practice as identified in this review and we will be sharing details of these operational provisions with other member authorities in the Consortium:

- Breckland is introducing payment for Members' expenses via iTrent, which is currently at trial and modification stage, with training to be set up for users of the system. This will reduce the need to submit manual claim forms and is accessible out of business hours.

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

- Current Members' allowances have been approved and published by both Councils, having considered outcomes of reviews by Independent Remuneration Panels. This is in accordance with the requirements of Statute, in particular, Local Government, England - The Local Authorities (Members' Allowances) (England) Regulations 2003.

- Checks are applied to confirm that members have attended the required number of Committee meetings to receive the basic rate allowance and special responsibility allowances. This demonstrates that only valid allowances are paid.

ISSUES TO BE ADDRESSED

The audit has highlighted the following areas where six 'important' recommendations have been made.

Training

- There is a need to produce an annual Member training programme that allows Members to know and plan for training opportunities which could otherwise be missed, thereby adversely impacting on the ability to discharge their duties more effectively. (South Holland)

- Members from both Councils to complete the GDPR training via e-learning and for GDPR training to be included in Members' induction training as standard. This is to reduce the risk that key principles will be overlooked, leading to reputational damage to the Members and the Council. (Both Councils)

Members' Expenses

- There is a need to document checks applied to Members' expense claim forms, so as to reduce the risk of inaccurate or unjustified expenses being paid, ultimately resulting in financial loss to the Council. (South Holland)

- There is a need for an improved audit trail in the submission and processing of Members expenses, to avoid the risk on non-compliance with the requirements of the Constitution and concerns with late payment of expenses, possibly resulting in late or incorrect and or fraudulent claims being paid. (South Holland)

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

Training

- For training on Governance and Standards and Code of Conduct to be included in annual Member Training Programmes and for such training to be mandatory, in order to reduce the risk of criticism for not acknowledging / complying with such requirements. (Both Councils).

Members' Allowances

- There is a need for the Council to publish allowances paid to its Members for 2017/18, in order to reduce the risk of non- compliance with the Local Authorities (Members' Allowances) (England) Regulations 2003 and the risk of reputational damage for the lack of transparency. (South Holland)

Members' Expenses (and Training)

- The Council to use one style of claim form for claiming Member expenses and that all forms show details of the authorising officer, thereby reducing the risk of claims not being authorised potentially resulting in claims being processed that do not meet the correct criteria. (South Holland)

Operational Effectiveness Matters

The operational effectiveness matters, for management to consider relate to the following:

- To consider updating the published scheme of Members' Allowances to provide more detail over allowances applicable for each category of Member responsibility, in particular, those receiving Special Responsibility Allowance. (South Holland)

- To consider the use of iTrent for claiming Members' expenses, to reduce manual processes and align with the Council's digital agenda. (South Holland)

Previous audit recommendations

This area has not been subject to previous audit scrutiny at South Holland by TIAA. A review of Democratic Services (BRK/16/06) was completed as part of the 2015/16 audit plan for Breckland DC, with the final report being issued in October 2015. The audit concluded in a 'Substantial' assurance opinion, with no recommendations being raised.

Maturity Assessment of Cyber Security

Executive Summary

OVERALL ASSURANCE ASSESSMENT

- SUBSTANTIAL ASSURANCE
- REASONABLE ASSURANCE
- LIMITED ASSURANCE
- NO ASSURANCE

ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Removable Media Controls	0	2	0	0
Incident Management	0	3	0	0
Total	**0**	**5**	**0**	**0**

SCOPE

This assessment has focussed on the National Cyber Security Centre's 10 steps to Cyber Security framework that covers Risk Management Regime, Network Security, User Education and Awareness, Malware Prevention, Removable Media Controls, Secure Configuration, Managing User Privileges, Incident Management, Home and mobile working and Monitoring.

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 an assessment of their maturity in the following recognised areas of Cyber Security:

    - Risk Management Regime;
    - Network Security
    - User Education and Awareness
    - Malware Prevention
    - Removable Media Controls
    - Secure Configuration
    - Managing User Privileges
    - Incident Management
    - Home and mobile working
    - Monitoring

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. The consistent level of Cybercrime is evidenced by the Police recorded crime statistics and the Crime Survey for England and Wales for the year ending March 2018. These figures highlight an increase of approximately 9% overall in computer-related crime to the year ending in March 2018 as compared to the previous year.

	Apr '16 to Mar '17	Apr '17 to Mar '18
Computer misuse crime	**19,376**	**21,134**
Computer viruses/malware	7,249	6,691
Denial of service attack	363	311
Denial of service attack (extortion)	416	260
Hacking - server	674	689
Hacking - personal	3,594	3,744
Hacking - social media and email	5,475	8,096

Hacking - PBX/dial through	507	311
Hacking (extortion)	1,098	1,032

4. Whilst the figures suggest a reduction in reported incidents relating to Computer Viruses and malware, there is a marked increase of 48% in the figures for Hacking – social media and email, suggesting a need for greater emphasis on raising the awareness of staff.

5. The new UK Data Protection Act 2018 that has incorporated the new General Data Protection Regulations (GDPR) 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 Information Commissioners Office (ICO) can now impose fines of up to 4% of annual turnover for breaches of the new UK Data Protection Act. Apart from the financial penalties, there could be extensive and very unwelcome reputational damage resulting from breaches.

6. This review took the form of a Maturity Assessment following up the previous full Cyber Security audit conducted in August and September 2016 (SH1712) with some compliance testing to verify the current status being suggested.

7. A maturity assessment revisits the original scope and performs a gap analysis between the original audit and the present.

8. Suggested scores for each of the scope areas achieved for the original audit were agreed and used as the baseline for the maturity assessment. An aspirational score for each area was also agreed and has been included in the assessment.

9. In the process of assessing maturity we have identified the current maturity level for each of the ten areas and ascertained management's aspirations and appetite for improvement to manage and mitigate risk.

10. Our Cyber Maturity model is based on the traditional maturity model, and comprises of levels 0-5 as described below:

- 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 (Performed) – Direction has been given by formal policy statements in this area covering expectations for management and operation.
- 2 (Managed) – The process stated in the policy is now implemented in a managed fashion, and its Cyber Security functionalities are formally addressed with procedure and processes in place.
- 3 (Established) – The managed process is now implemented using a formal procedure that is capable of achieving its Cyber Security outcomes.
- 4 (Predictable) – The established process can now be put into action and tested thoroughly for better outcome.
- 5 (Optimizing) – The predictable process is continuously improved according to how cyber threats change and how business needs change.

SUMMARY

11. Our review noted that management rated South Holland District Council's (SHDC) dependency on Information technology as High and recognised that Cybercrime was a significant risk. Management considered that untreated cyber risks were at a Medium level. It was noted that the organisation had invested in improving cyber security measures in the last 12 months.

12. SHDC last experienced a cyber incident in 2015 and was caused by a Ransomware attack that affected a network share for around two hours. A network share is typically defined as an area of the network accessible by one or more departments for saving and retrieving data. The previous day's backup was used to restore the data stored in the network share. This incident had a Medium impact on the organisation, and recovery was achieved within one day. The incident was formally investigated and reported upon, with a range of control improvements being implemented as a result. There have not been any similar events since that time.

13. Our maturity assessment is summarised in the radar diagram below. Significant gaps or 2 or more maturity steps between the aspirational level of maturity and the current assessed level was noted for the following process area: "Removable Media Controls" and "Incident Management".
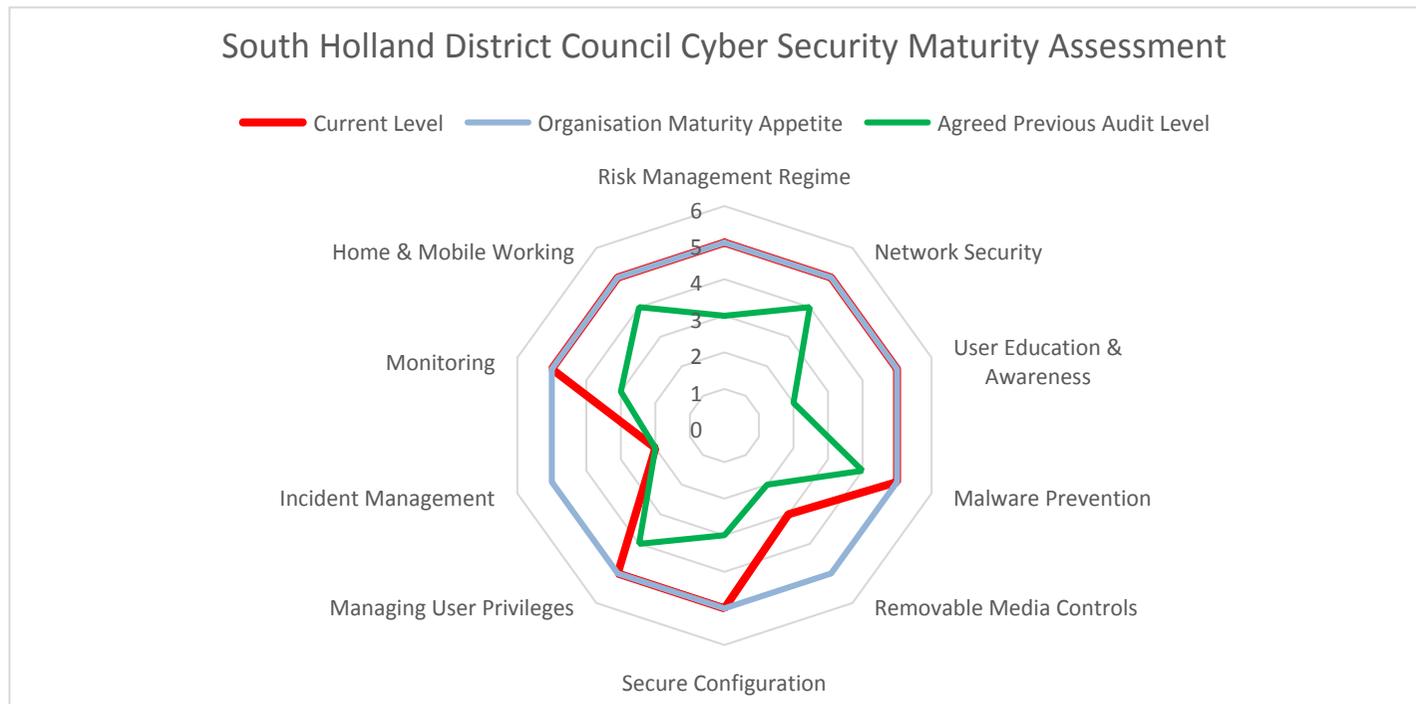
14.   Where gaps have been identified management should consider our maturity improvement recommendations within this report. In order to achieve maturity improvement, the two maturity steps below require early action to help realise the aspirations of the Council, working with Compass Point Business Services (East Coast) Ltd.

Rec.	Cyber Area	Finding	Recommendation	To Achieve Maturity Level
RMC 4	Removable Media Controls	Level 4 maturity is not fully achieved.	To achieve level 4, monitoring must be carried out on the use of removable media, including high risk events that involve the removal of sensitive data. Results of the monitoring must be reported to senior management.	4
IM 3	Incident Management	Level 3 maturity is not fully achieved.	To achieve level 3 a forensics readiness approach must be implemented for implementation and management of the organisation's digital systems and staff responsible for responding to incidents must be trained in the process. An established incident response capability must be in place and tested alongside a data recovery capability.	3

Assurance Review of the Software Licencing

Executive Summary

OVERALL ASSURANCE ASSESSMENT

REASONABLE ASSURANCE

- SUBSTANTIAL ASSURANCE
- REASONABLE ASSURANCE
- LIMITED ASSURANCE
- NO ASSURANCE

ACTION POINTS

Control Area	Urgent	Important	Needs Attention	Operational
Software Policies	0	1	0	0
Software Inventory	0	0	0	1
Software Copyright	0	0	0	1
Total	0	1	0	2

No recommendations arose in the areas of Security of Software media and licenses and Software Licence Procurement.

SCOPE

The corporate objectives for the service are to ensure that the controls in place to manage Software Licensing are operating securely and effectively. Key software vendors such as Microsoft and Adobe conduct periodic audits of their clients to understand how well their respective products are being licensed. Weak software licensing could result in punitive and reputational damage. The audit covered the following: Software Policies; Software Inventory; Security of Software media and licenses (where appropriate); Software Copyright; and Software Licensing Procurement.

RATIONALE

- The systems and processes of internal control are, overall, deemed 'Reasonable Assurance' in managing the risks associated with the audit. The assurance opinion has been derived as a result of one 'Important' recommendation being raised upon the conclusion of our work.

- The audit has also raised two 'Operational Effectiveness Matters', which sets 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.

POSITIVE FINDINGS

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

- The Compass Point "Acceptable Use Policy" contains several policy requirements that relate to Software usage and consequences for breaching the policy..

- Compass Point uses a software monitoring tool known as Snow for the management of software assets. The tool receives data from Snow agents that are installed on relevant server and client machines. The agents report on the software installed on their respective machines and keep a record of the average time spent using each software asset on the machine.

- There are periodic reviews of agent installations to verify that all machines that require them have had them installed. The installation of the agents is handled automatically by Active Directory Group Policy, although there are occasions where the installation is not completed, hence the periodic review that is undertaken to capture those machines and resolve the discrepancy.

- The Snow software management system effectively acts as a continuous auditing system as it keeps itself updated on actual software numbers in use on a daily basis. Key software licence details are manually recorded within Snow and are then used to compare actual usage against availability. Some systems, such as the anti-virus solution, automatically monitor licence usage themselves, which acts as an additional control.

- It was found that software installation files are stored within files secured by Administrator level privileges.

- Licence procurement and payments for licence renewals is managed by the Compass Point IT department. . Initial 'one-off' licences are purchased using the relevant department budget with any renewals being covered by the IT Department. The annual Microsoft Enterprise Agreement true up process was confirmed as completed in February 2018. This process is an annual 'correction' of the number of Microsoft Licences being used by the Council and is an example of the flexibility that Enterprise Agreements have.

- Snow is used to assist with the discovery of unused software and transfer it to other users that request it rather than purchasing an additional copy.

- The Council is migrating to Office 365 during 2019, which will change the way that part of the Microsoft Enterprise Agreement operates from a licencing perspective. It was also noted that there is governance over any requests for major changes to software in place, such as changes to service area applications. An example of this is APP Flare.

ISSUES TO BE ADDRESSED

The audit has highlighted the following areas where one 'Important' recommendation has been made.

Software Policies

- There is a need to ensure that Software Asset Management policies and procedures are formally documented and approved to facilitate a more consistent approach to this area.

Operational Effectiveness Matters

The operational effectiveness matters, for management to consider relate to the following:

- Consideration to be given to implementing a process whereby all software with more than 60 licences be kept aligned more closely to the actual number of licences available within Snow. At present, software with a smaller number of licences are not kept fully aligned to actual licence usage for practical operational reasons.

- Consideration to be given to conducting further 'friendly' software audits such as that performed by TrustMark in 2014 to help demonstrate an independent view of licencing compliance.