REPORT TO: **TAYSIDE VALUATION JOINT BOARD – 24 AUGUST 2020**

REPORT ON: **INTERNAL AUDIT**

REPORT BY: **ASSESSOR**

REPORT NO: **TVJB 9-2020**

1 PURPOSE OF REPORT

1.1 To present to the Board the following Internal Audit Reports, together with the Internal Audit Annual Plan for 2020/21, which are attached as appendices to this report,:-

Internal Audit Report – 2020/05 - IT Network Arrangements / Cyber Security
Internal Audit Report – 2020/06 - Follow-Up Reviews
Internal Audit Report – 2020/07 - Annual Report 2019/20
Internal Audit Plan – 2021/01 - Annual Plan 2020/21

2 RECOMMENDATIONS

2.1 The Board is asked to note the contents of the three Audit Reports and approve the Internal Audit Annual Plan for 2020/21.

3 FINANCIAL IMPLICATIONS

3.1 The cost of Internal Audit Services is provided for in the Assessor's Revenue Budget.

4 POLICY IMPLICATIONS

4.1 This report has been screened for any policy implications in respect of Sustainability, Strategic Environmental Assessment, Anti Poverty, Equality Impact Assessment and Risk Management. There are no major issues.

5 BACKGROUND

5.1 Henderson Loggie, Chartered Accountants, were appointed to provide an Internal Audit Service in respect of the financial years 1 April 2019 to 31 March 2022. Audit work has proceeded in accordance with the Audit Needs Assessment and Strategic Plan for the period 2019 to 2022 as approved by the Joint Board on 26 August 2019.

5.2 Internal Audit Report No. 2020/05 - IT Network Arrangements / Cyber Security - is attached as Appendix 1 to this report. It has been prepared by Internal Audit following discussion with the Assessor and relevant members of staff. The overall conclusion of the review is that the level of assurance is satisfactory and that the system meets the control objectives with some weaknesses present. Internal Audit have made four recommendations for system improvements relating to intrusion detection & prevention systems, system auto-run facilities and security training. Management will investigate remedial actions that may be taken to address these issues and, where appropriate, will seek external advice.

5.3 Internal Audit Report No. 2020/06 – Follow-Up Reviews - is attached as Appendix 2 to this report. It has been prepared by Internal Audit following discussion with the Assessor and relevant members of staff. This review assessed whether recommendations made in previous Internal Audit reports have been appropriately implemented. The overall conclusion of the review is that the Board has made

progress in fully implementing three of the eight recommendations followed up as part of this review. Of the remaining five recommendations, two relate to requested enhancements to the electoral registration management system, which the system vendor has confirmed that it would not be viable to introduce. These recommendations were therefore not implemented. Three recommendations relate to project management for which no opportunities have arisen which would require a project management methodology to be applied. It was agreed to remove these recommendations and project management controls will be reviewed further as part of future audits.

5.4 Internal Audit Report No. 2020/07 – Annual Report to the Joint Board and the Assessor - is attached as Appendix 3 to this report. It sets out a summary of the audit reviews undertaken during the year 2019/20 and the results and conclusions of those reviews. The overall conclusion of the report is that the Board operates adequate internal control systems as defined in the Audit Needs Assessment. The audit and assurance work has not identified any significant gaps in the Board's control environment that would increase the risk of financial loss.

5.5 The Internal Audit Annual Plan 2020/21 (No. 2021/01) is attached as Appendix 4 to this report. It sets out the scope and objectives for assignments which will be carried out by Internal Audit during the year 2020/21. At the conclusion of each assignment a detailed report will be made to the Board. The assignments include:

- Compliance with Legislation
- Maintenance of the Valuation Roll
- Corporate Governance
- Follow-Up Reviews

6 CONSULTATIONS

6.1 The Clerk and Treasurer to the Board have been consulted on this report.

7 BACKGROUND PAPERS

7.1 None.

ALASTAIR KIRKWOOD
Assessor **August 2020**

APPENDIX 1

Tayside Valuation Joint Board

IT Network Arrangements / Cyber Security

Internal Audit Report No: 2020/05

Draft issued: 21 July 2020

Final issued: 24 July 2020

LEVEL OF ASSURANCE	Satisfactory

Now, for tomorrow

mha HENDERSON LOGGIE

Contents

		Page No.
Section 1	**Management Summary**	
	• **Overall Level of Assurance**	**1**
	• **Risk Assessment**	**1**
	• **Background**	**1**
	• **Scope, Objectives and Overall Findings**	**2**
	• **Audit Approach**	**2**
	• **Summary of Main Findings**	**3**
	• **Acknowledgements**	**3**
Section 2	**Main Findings and Action Plan**	**4 - 9**
Appendix I	**NCSC 10 Steps to Cyber Security**	**10**

Level of Assurance

In addition to the grading of individual recommendations in the action plan, audit findings are assessed and graded on an overall basis to denote the level of assurance that can be taken from the report. Risk and materiality levels are considered in the assessment and grading process as well as the general quality of the procedures in place.

Gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the organisation to material risk and which requires to be brought to the attention of management and the Joint Board.
Priority 2	Issue subjecting the organisation to significant risk and which should be addressed by the Assessor.
Priority 3	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

Management Summary

Overall Level of Assurance

Satisfactory	System meets control objectives with some weaknesses present

Risk Assessment

This review focused on the controls in place to mitigate the following risks on the Tayside Valuation Joint Board ('the Board') Risk Register:

3.2 Malicious damage to systems (risk rating: low)
3.3 Attempted breach of security (risk rating: low)
3.8 Inappropriate use of Internet/Email by staff (risk rating: low)
6.3.1 Loss of IT capability (Electoral Registration) (risk rating: low)

Background

As part of the Internal Audit programme at the Board for 2019/20 we carried out a review of the organisation's IT network and cyber security arrangements. Our Audit Needs Assessment identified this as an area where risk can arise and where Internal Audit can assist in providing assurances to the Assessor and the Joint Board that the related control environment is operating effectively, ensuring risk is maintained at an acceptable level.

Responsibility for ensuring an efficient and effective IT service delivery to all staff and other service users lies with the IT Department. This includes first level support over some of the main application systems used in the provision and maintenance of user access to the network. The IT Department is also responsible for purchasing and maintaining the servers upon which the applications are housed; the desktop computers and mobile devices used by staff; and the network which connects them.

The Board has deployed significant resources in developing, acquiring, and maintaining application and business systems. In turn, these systems manage critical information and should be considered an asset that requires to be effectively managed and controlled.

Scope, Objectives and Overall Findings

This audit included a review of the Board's current position regarding IT Security in order to advise on areas that should be addressed in line with the latest guidance produced by National Cyber Security Centre (NCSC), the UK Government's national technical authority for cyber security.

The table below notes the objectives for this review and records the results:

Objective	Findings			
The specific objective of this audit was to:		**1**	**2**	**3**
1. Review the internal controls in place which ensure the security of the IT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users. This covered the following areas: • Information risk management. • Secure configuration of ICT equipment. • Network security. • Managing user privileges. • ICT user education and awareness. • Incident management (including disaster recovery). • Malware prevention. • Monitoring. • Removable media controls; and • Home and mobile working.	**Satisfactory**	0	1	3
Overall Level of Assurance	**Satisfactory**	**0**	**1**	**3**
		System meets control objectives with some weaknesses present		

Audit Approach

Based upon the guidance and best practice provided by the NCSC; we reviewed the achievement of the above objective through discussion with the IT Development Manager and other members of the IT team and through review of relevant documentation and systems reports.

Summary of Main Findings

Overall, the Board demonstrated a strong awareness of the risks of information / cyber security, which is reflected in the control environment that demonstrates good practice in most areas.

Strengths

- A risk management regime has been established, which includes identifying information / cyber security as key strategic risks and establishing an IT security policy set to mitigate those risks.
- A baseline security build for network infrastructure is in place.
- Hardware and software inventories have been created.
- Processes are in place for applying updates and patches to all devices connected to the IT network.
- The IT architecture protects the organisation's network through use of firewalls and segregation controls which prevent direct connections to untrusted external services and protects internal IP addresses.
- Management of user accounts is linked to the organisation's new staff starter, leaver and change of role procedures.
- Network hardware is protected by an antivirus solution, which automatically scans for malware.
- Whitelisting of removable media is in place and devices are scanned for malware when connected to networked equipment.
- The Board has achieved the Cyber Essentials certification, which demonstrates a clear commitment to cyber risk management.
- The Board's network also connects to, and forms part of, the UK Government's Public Services Network (PNS). The PNS is responsible for overseeing and managing the PSN compliance process ensuring that organisations that connect to the PNS are adequately secured. As part of this process, the PNS undertakes an annual health check of the Board's network security.

Weaknesses

- It is good practice for an organisation to run automated vulnerability scanning tools against all networked devices regularly and to remedy any identified vulnerabilities within an agreed time frame. We noted that the Board engages with a third-party to provide a vulnerability management service which provides scanning and triage reporting of vulnerabilities on a limited number of network devices only.
- As part of a layered approach to network security, where possible, the auto run function should be disabled on devices to prevent the automatic import of malicious code from any type of removable media. Equally, if removable media is introduced, the system should automatically scan it for malicious content. We note that although tools are in place which automatically scan removable media autorun has not been disabled.
- Our review found that although IT staff demonstrated a strong awareness of information security risks, and the dangers of phishing and malware are communicated to staff, the organisation is not yet in a position to demonstrate that the same level of awareness exists amongst the wider staff group as currently there is no structured programme of information security training provided to staff or any mechanism for testing the effectiveness of training provided.

Acknowledgements

We would like to take this opportunity to thank the staff who helped us during our audit.

Main Findings and Action Plan

Objective 1: Review the internal controls in place which ensure the security of the IT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users. This will cover the following areas:

- **Information risk management.**
- **Secure configuration of ICT equipment.**
- **Network security.**
- **Managing user privileges.**
- **ICT user education and awareness.**
- **Incident management (including disaster recovery).**
- **Malware prevention.**
- **Monitoring.**
- **Removable media controls; and**
- **Home and mobile working.**

The NCSC's 10 Steps to Cyber Security guidance sets out what a common cyber-attack looks like and how attackers typically undertake them. Understanding the cyber and information security environment and adopting an approach aligned with the NCSC's 10 Steps is an effective means to help protect the organisation from cyber-attacks.

Information Risk Management

Defining and communicating the Board's information risk management regime should be a central pillar of the Board's overall cyber security strategy. The NCSC recommends that organisations should review this regime, together with the nine associated security areas described in Appendix I, to protect against most cyber-attacks.

IT Network Arrangements / Cyber Security

Objective 1: Review the internal controls in place which ensure the security of the IT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

Information Risk Management (continued)

To be fully effective an information risk management regime should be supported by an empowered governance structure, which is actively supported by the Joint Board and senior managers. Our review identified that there are groups in place which act as appropriate bodies for evaluating and monitoring information security risks within the organisation.

At a corporate level, a risk management regime has been established with a strategic risk register, which identifies data, information, and cyber security as key risks, monitored by the Joint Board and management. IT operational risks, including cyber security risks, are monitored by the IT team. The Board's Business Continuity Plan, Risk Management Strategy, Risk Register, and suite of IT Data Access & Security Policies combine to communicate and support risk management objectives, setting out the information risk management strategy for the Board.

Objective 1: Review the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

Observation	Risks	Recommendation	Management Response	
Network Security It is good practice for an organisation to run automated vulnerability scanning tools against all networked devices regularly and remedy any identified vulnerabilities within an agreed time frame. We noted that at the time of our audit an Intrusion Detection System (IDS) or Intrusion Prevention System (IPS) were not deployed on the IT network. Though they both relate to network security, IDS differs from a firewall in that a firewall looks outwardly for intrusions in order to stop them from happening. Firewalls limit access between networks to prevent intrusion and do not signal an attack from inside the network. An IDS evaluates a suspected intrusion once it has taken place and signals an alarm. An IDS also watches for attacks that originate from within a system. A system that terminates connections is called an IPS, and is another form of an application layer firewall. We noted that the Board engages with a third-party to provide a vulnerability management service which provides scanning and triage reporting of vulnerabilities on a limited number of network devices only. The Board's network also connects to, and forms part of, the UK Government's Public Services Network (PNS). The PNS is responsible for overseeing and managing the PSN compliance process ensuring that organisations that connect to the PNS are adequately secured. As part of this process the PNS undertakes an annual health check of the Board's network security.	Unusual or malicious network traffic or incoming and outgoing activity that could indicate an attack (or attempted attack) is not identified.	**R1** Tools such as network intrusion detection and network intrusion prevention should be placed on the network and configured to monitor traffic for unusual or malicious incoming and outgoing activity that could be indicative of an attack or an attempt. Alerts generated by the system should be promptly managed by IT staff, trends analysed and where significant security issues are identified these are reported to management.	Management will investigate the availability of suitable Intrusion Detection and Intrusion Prevention systems which are compatible with existing network arrangements. **To be actioned by:** IT Manager **No later than:** 31 March 2021	
			Grade	**3**

Objective 1: Review the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).				
Observation	**Risks**	**Recommendation**	**Management Response**	
Malware Prevention As part of a layered approach to network security, where it is practical to do so, the auto run function should be disabled on devices to prevent the automatic import of malicious code from any type of removable media. Equally, if removable media is introduced, the system should automatically scan it for malicious content. We note that although tools are in place which automatically scan removable media autorun has not been disabled.	Removable media is a popular attack vector for introducing malicious programmes into the computer network.	**R2** Consider disabling the autorun facility on all networked devices.	The auto run facility will be disabled. **To be actioned by:** IT Manager **No later than:** 30 August 2020	
			Grade	**3**

Objective 1: Review the internal controls in place which ensure the security of the IT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).

User Education and Awareness

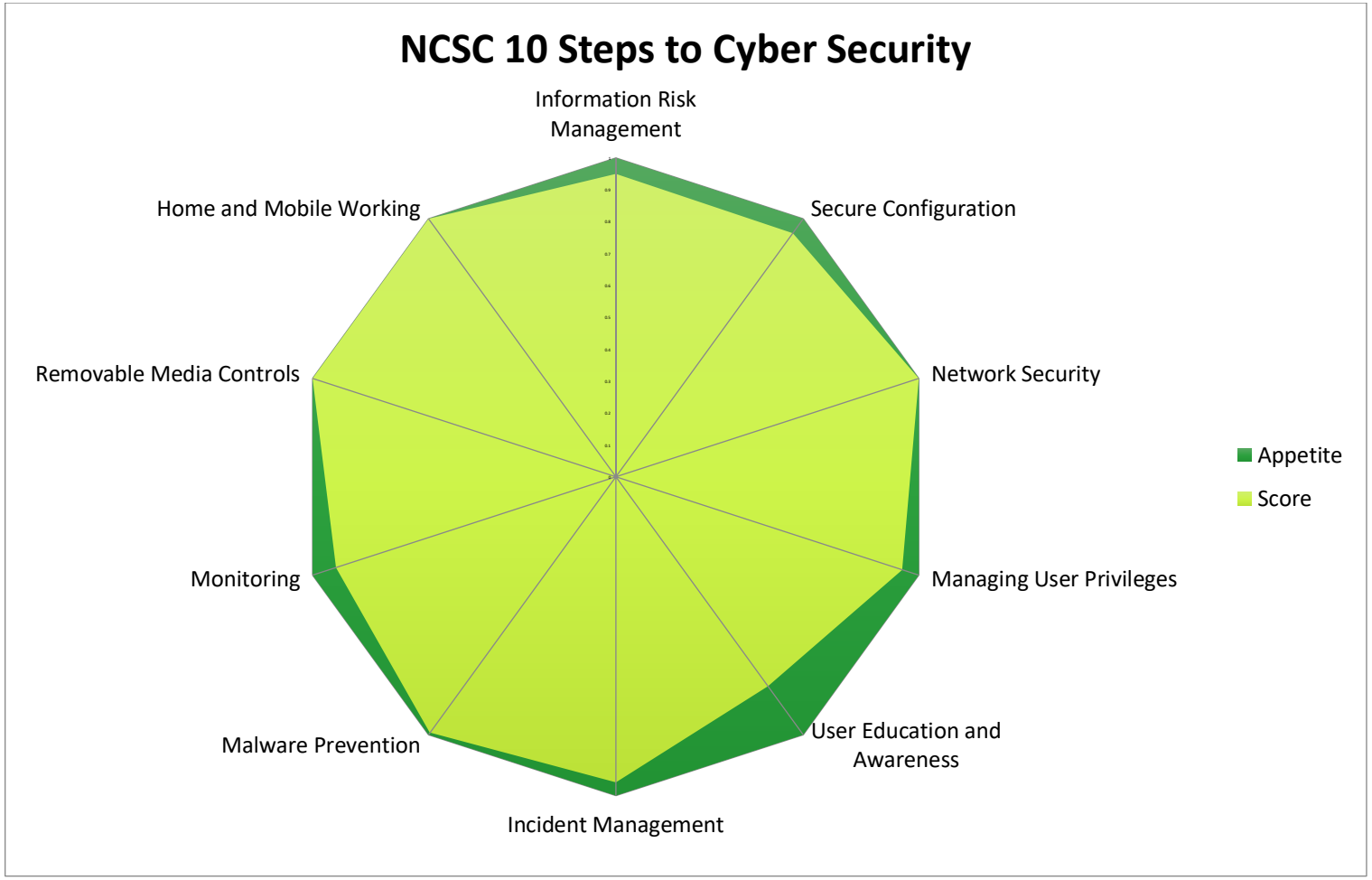
Users have a critical role to play in the organisation's security and so it is important that security rules and the technology provided enables users to do their job as well as help keep the organisation secure. This can be supported by a systematic delivery of awareness programmes and training that deliver security expertise as well as helping to establish a security-conscious culture.

Observation	Risks	Recommendation	Management Response	
Our review identified that although IT staff demonstrated a strong awareness of information security risks the Board as an organisation is unable to demonstrate that the same level of awareness exists amongst the wider staff and user groups as currently there is no structured programme of information security training provided to staff. It is good practice for a programme of mandatory refresher training where the frequency and level of training required for each job role is based on a risk assessment, linked to staff exposure to systems and data. Information security guidance is made available on the internal computer network, which is signposted during the induction process for new staff, however there is scope for further promoting this to all staff. The induction process for new staff includes mandatory IT / cyber security training. Information on phishing and malware is regularly communicated by IT to staff. Members of the IT team are suitably qualified and experienced however do not hold any recognised information assurance certifications. Staff in security roles should be encouraged to develop and formally validate their information assurance skills through enrolment on a recognised certification scheme.	Organisations that do not effectively support employees through education and awareness may be vulnerable to a range of risks, including: • introduction of malware and data loss through use of removable media. • legal sanctions due to loss of sensitive data. • external attacks due to email phishing and social engineering; and • data loss or corruption due to an internal attack by a dissatisfied employee.	**R3** Develop a programme of information security training for new and existing staff to mitigate information security risks, covering: • the Board's IT security policies and procedures. • cyber security risks and strategies for defence, covering internet safety, mobile and home working, phishing, and prevention against malware. • regular refresher training on the security risks to the organisation. • supporting staff in information security roles to enrol on a recognised certification scheme. • monitoring the effectiveness of security training; and • promoting an incident reporting culture.	Management will investigate whether a suitable programme of information security training for existing staff can be sourced externally or developed internally. Consideration will be given to the availability of suitable certification-based training for staff in security roles. **To be actioned by:** IT Manager **No later than:** 30 June 2021	
			Grade	**2**

Objective 1: Review the security tools in place, how these are currently used, the configuration of key elements of IT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users (continued).				
Observation	**Risks**	**Recommendation**	**Management Response**	
As above.	As above.	**R4** Once training has been delivered (**R3**) establish mechanisms to test the effectiveness and value of the security training provided to staff. Those areas of the organisation that regularly feature in security reports or achieve the lowest feedback from information security questionnaires should be targeted for further tailored training.	Management will investigate the availability of mechanisms to test the effectiveness of security training provided to staff. Any resultant feedback will be utilised to target further tailored training. **To be actioned by:** IT Manager **No later than:** 30 June 2021	
			Grade	**3**

Appendix I – NCSC 10 Steps to Cyber Security

The Graphic below illustrates the organisation's current position, based on our assessment, in relation to the NCSC's 10 Steps to Cyber Security guidance.



Aberdeen

45 Queen's Road
Aberdeen
AB15 4ZN

T: 01224 322100

Dundee

The Vision Building
20 Greenmarket
Dundee
DD1 4QB

T: 01382 200055

Edinburgh

Ground Floor
11-15 Thistle Street
Edinburgh
EH2 1DF

T: 0131 226 0200

Glasgow

100 West George Street
Glasgow
G2 1PP

T: 0141 471 9870

mha HENDERSON LOGGIE

hlca.co.uk | info@hlca.co.uk

APPENDIX 2

Tayside Valuation Joint Board

Follow-Up Reviews

2019/20

Internal Audit Report No: 2020/06

Draft issued: 21 July 2020

Final issued: 24 July 2020

Contents

	Page No.
1. Management Summary	**1 - 4**
• **Introduction and Background**	**1**
• **Audit Scope and Objectives**	**1**
• **Audit Approach**	**1**
• **Overall Conclusion**	**2 - 4**
• **Acknowledgements**	**4**

Appendices

Appendix I	**Updated Action Plan: Internal Audit Report 2019/02 – Risk Management / Business Continuity**	**5**
Appendix II	**Updated Action Plan: Internal Audit Report 2019/04 – Maintenance of Accuracy of the Electoral Register**	**6 - 7**
Appendix III	**Updated Action Plan: Internal Audit Report 2019/05 – Follow-Up Reviews 2018/19**	**8 - 11**

1. Management Summary

Introduction and Background

We have been appointed as Internal Auditors to the Tayside Valuation Joint Board ('the Board') for the period 1 April 2019 to 31 March 2022. The Internal Audit Plan for 2019/20 includes time for follow-up work on the recommendations made in our Internal Audit reports issued during 2018/19. These were:

2019/02 – Risk Management / Business Continuity Planning;
2019/04 – Maintenance of Accuracy of the Electoral Register; and
2019/05 – Follow-Up Reviews.

Reports 2019/01, 2019/03 and 2019/06 did not contain an action plan and therefore no follow-up was required as part of this review.

Report 2019/05 included one outstanding recommendation from 2017/18, two outstanding actions from 2014/15 and one from 2010/11 that required to be followed up again this year.

Audit Scope and Objectives

The objective of our follow-up review is to assess whether recommendations made in internal audit reports from 2018/19, and previous years, have been appropriately implemented and to ensure that, where little or no progress has been made towards implementation, that plans are in place to progress them.

Audit Approach

The audit approach taken was as follows:

- to request from responsible officers for each report listed above an update on the status of implementation of the recommendations made;
- to ascertain by review of supporting documentation, for any significant recommendations within the reports listed above, whether action undertaken has been adequate; and
- preparation of a summary of the current status of the recommendations for the Board.

Overall Conclusion

The Board has made progress in fully implementing three of the eight recommendations followed up as part of this review. The remaining five recommendations have been considered by management but not implemented, including:

- two recommendations raised in internal audit report 2019/04 – Maintenance of Accuracy of the Electoral Register – where, following further review, the system vendor confirmed that it would not be viable to incorporate the audit recommendations into the system; and
- three recommendations which were raised in reports in 2010/11 and 2014/15 relating to project management. As no opportunities have arisen, or are likely to arise in the foreseeable future, which would require a project management methodology to be applied it was agreed with the Assessor to remove these recommendations. Project management controls will be reviewed as part of future relevant audits.

2018/19

From Original Reports			*From Follow-Up Work Performed*			
Area	**Rec'n Grades**	**Number Agreed**	**Fully Implemented**	**Partially Implemented**	**Little or No Progress Made**	**Considered But Not implemented**
Risk Management / Business Continuity	1	-	-	-	-	-
	2	-	-	-	-	-
	3	1	1	-	-	-
Total		**1**	**1**	**-**	**-**	**-**
Maintenance of Accuracy of the Electoral Register	1	-	-	-	-	-
	2	-	-	-	-	-
	3	3	1	-	-	2
Total		**1**	**1**	**-**	**-**	**2**
Overall Total 2018/19		**4**	**2**	**-**	**-**	**2**

2017/18

From Original Reports			*From Follow-Up Work Performed*			
Area	**Rec'n Grades**	**Number Agreed**	**Fully Implemented**	**Partially Implemented**	**Little or No Progress Made**	**Considered But Not Implemented**
Corporate Governance	1	-	-	-	-	-
	2	-	-	-	-	-
	3	1	1	-	-	-
Total 2017/18		**1**	**1**	**-**	**-**	**-**

Overall Conclusion (continued)

2014/15

From Original Reports			*From Follow-Up Work Performed*			
Area	**Rec'n Grades**	**Number Agreed**	**Fully Implemented**	**Partially Implemented**	**Little or No Progress Made**	**Considered But Not Implemented**
Risk Management and Business Continuity	A	-	-	-	-	-
	B	-	-	-	-	-
	C	1	-	-	-	1
Total		**1**	**-**	**-**	**-**	**1**
IT Network Arrangements	A	-	-	-	-	-
	B	1	-	-	-	1
	C	-	-	-	-	-
Total		**1**	**-**	**-**	**-**	**1**
Overall Total 2014/15		**2**	**-**	**-**	**-**	**2**

2010/11

From Original Reports			*From Follow-Up Work Performed*			
Area	**Rec'n Grades**	**Number Agreed**	**Fully Implemented**	**Partially Implemented**	**Little or No Progress Made**	**Considered But Not Implemented**
Systems Development	A	-	-	-	-	-
	B	1	-	-	-	1
	C	-	-	-	-	-
Total 2010/11		**1**	**-**	**-**	**-**	**1**
Grand Total		**8**	**3**	**-**	**-**	**5**

Overall Conclusion (continued)

The grades, as detailed below, denote the level of importance as they relate to each individual recommendation:

Reports issued since 2016/17:

Priority 1	Issues which require the consideration of the Joint Board.
Priority 2	Significant matters which the Assessor can resolve.
Priority 3	Less significant matters, which do not require urgent attention, but which should be followed up within a reasonable timescale.

Reports issued prior to 2015/16:

A Issues which require the consideration of the Joint Board.

B Significant matters which can be resolved by the Assessor.

C Less significant matters, which do not require urgent attention, but which should be followed up within a reasonable timescale.

Acknowledgments

We would like to take this opportunity to thank the staff at the Board who assisted us during our review.

Appendix I - Updated Action Plan: Internal Audit Report 2019/02 – Risk Management / Business Continuity

Recommendation	Grade	Management Response	Agreed Y/N	Responsible Officer For Action	Agreed Completion Date	Progress at June 2020
R1 Ensure that the findings and conclusions of testing of the IT Disaster Recovery Plan are formally recorded and where required, results are used to amend the plan to ensure it remains workable.	**3**	Indicators to be identified and embedded within performance management through inclusion in objectives for 2020.	Yes	IT Manager	31 March 2019	The findings and conclusions of the testing of the IT Disaster Recovery Plan are formally recorded and, where appropriate, results will be used to inform future actions. ***Fully Implemented***

Appendix II - Updated Action Plan: Internal Audit Report 2019/02 – Maintenance of Accuracy of Electoral Register

Recommendation	Grade	Management Response	Agreed Y/N	Responsible Officer For Action	Agreed Completion Date	Progress at June 2020
R1 Investigate how the EROS system can be developed to provide an enhanced audit trail of the secondary checking of processed batches.	**3**	Agreed. The benefit of electronically recording secondary checks is recognised. Approaches will be made to the system vendor to ascertain whether this functionality can be provided.	Yes	Administration Manager (ER/Clerical)	31 December 2019	The system vendor has confirmed that it would not be viable to incorporate these changes into the system which is provided to all clients across the UK. ***Considered But Not Implemented***
R2 Discuss with the EROS system vendor how the batch header sheets can be configured to include details of the users that upload the batches, process the batches and perform secondary checks. This would eliminate the need for manually printing and signing the header sheet and provide a full audit trail of checks to be retained within the system.	**3**	Agreed. The benefit of configuring batch header sheets to include details of users that upload batches, process batches and perform secondary checks is recognised. Approaches will be made to the system vendor to ascertain whether this functionality can be provided.	Yes	Administration Manager (ER/Clerical)	31 December 2019	The system vendor has confirmed that it would not be viable to incorporate these changes into the system which is provided to all clients across the UK. ***Considered But Not Implemented***

Recommendation	Grade	Management Response	Agreed Y/N	Responsible Officer For Action	Agreed Completion Date	Progress at June 2020
R3 If on investigation it is determined that the suggested system developments proposed at **R1** and **R2** cannot be implemented ensure that the physical copies of the signed batch header sheets are scanned and stored within the Board's systems as evidence of checks undertaken.	**3**	Agreed. If the above system enhancements cannot be provided a procedure will be implemented to ensure that the signed batch header sheets are scanned and stored within the Board's systems as evidence of the checks undertaken.	Yes	Administration Manager (ER/Clerical)	31 December 2019	A procedure has been introduced through which batch header sheets are initialled and dated by the individuals undertaking the scanning, processing and checking procedures. The batch header sheets are scanned and retained within the Board's systems as evidence of the checks undertaken. ***Fully Implemented***

Appendix III - Internal Audit Report 2019/05 – Follow-Up Reviews 2018/19

2019/03 – Corporate Governance				
Original Recommendation	**Grade**	**Management Response**	**Progress at June 2019**	**Progress at June 2020**
R1 Ensure that the Scheme of Delegation is reviewed and updated where applicable to reflect any changes in the Board's governance arrangements.	**3**	The Scheme of Delegation will be reviewed and updated. **To be actioned by:** Assessor, Treasurer, Clerk **No later than:** 30 September 2019	Scheme of Delegation still to be updated. A formal review is scheduled for later in 2019. **Revised completion date:** 31 December 2019 ***Little or No Progress Made***	Scheme of Delegation updated and reported to the Joint Board on 26 August 2019. ***Fully Implemented***

2015/03 – Risk Management and Business Continuity							
Recommendation	**Grade**	**Comments**	**Agreed**	**Responsible Officer**	**Agreed Completion Date**	**Progress Previously Reported**	**Progress at May 2020**
R11 Consider what project management and risk management processes should be put in place over projects.	C		Y	Chair of Governance Working Group September 2012	September 2012	**May 2017:** No projects of sufficient scale have recently been undertaken. Revised completion date: 31 March 2018 ***No Project To Trigger Action*** **May 2018:** No projects of sufficient scale have recently been undertaken, however projects are currently being considered for 2018/19 which may provide a suitable opportunity to apply a project management methodology. With this in mind senior managers received project management training during 2017. **Revised completion date:** 31 March 2019 ***Partially Implemented*** **June 2019:** No projects of sufficient scale have recently been undertaken. **Revised completion date:** 31 March 2020 ***Partially Implemented***	No projects of sufficient scale have recently been undertaken. No further opportunities for implementing a project management methodology are expected in the near future. Agreed with the Assessor that this recommendation will be removed and project management will be revisited as part of future relevant audits. ***Considered But Not Implemented***

2015/06 – IT Network Arrangements							
Recommendation	**Grade**	**Comments**	**Agreed**	**Responsible Officer**	**Agreed Completion Date**	**Progress Previously Reported**	**Progress at May 2020**
PSN Implementation R1 Ensure that for future IT projects suitable governance arrangements are put in place which clearly define aims, objectives, roles, responsibilities and timescales in relation to project management, monitoring and accountability.	B	Future IT projects which are of significant size will have suitable governance arrangements.	Yes	Assessor / IT Manager	As required.	**May 2017:** No projects of sufficient scale have recently been undertaken. Revised completion date: 31 March 2018 ***No Project To Trigger Action*** **May 2018:** No projects of sufficient scale have recently been undertaken, however projects are currently being considered for 2018/19 which may provide a suitable opportunity to apply a project management methodology. With this in mind senior managers received project management training during 2017. Revised completion date: 31 March 2019 ***Partially Implemented*** **June 2019:** No projects of sufficient scale have recently been undertaken. **Revised completion date:** 31 March 2020 ***Partially Implemented***	No projects of sufficient scale have recently been undertaken. No further opportunities for implementing a project management methodology are expected in the near future. Agreed with the Assessor that this recommendation will be removed and project management will be revisited as part of future relevant audits. ***Considered But Not Implemented***

2011/08 - Systems Development							
Recommendation	**Grade**	**Comments**	**Agreed**	**Responsible Officer**	**Agreed Completion Date**	**Progress Previously Reported**	**Progress at May 2020**
Project Management **R1** If large-scale projects are undertaken in future, consideration should be given to the training needs of the project manager and the project management tools to be employed for the project. This should cover all aspects of the implementation, including setting criteria for testing, user acceptance, training and criteria for assessing the post implementation stage.	B		Yes	Assessor	***Original*** On-going	**May 2017:** No projects of sufficient scale have recently been undertaken. Revised completion date: 31 March 2018 ***No Project To Trigger Action*** **May 2018:** No projects of sufficient scale have recently been undertaken, however projects are currently being considered for 2018/19 which may provide a suitable opportunity to apply a project management methodology. With this in mind senior managers received project management training during 2017. Revised completion date: 31 March 2019 ***Partially Implemented*** **May 2019:** No projects of sufficient scale have recently been undertaken. Revised completion date: 31 March 2020 ***Partially Implemented***	No projects of sufficient scale have recently been undertaken. No further opportunities for implementing a project management methodology are expected in the near future. Agreed with the Assessor that this recommendation will be removed and project management will be revisited as part of future relevant audits. ***Considered But Not Implemented***

Aberdeen

45 Queen's Road
Aberdeen
AB15 4ZN

T: 01224 322100

Dundee

The Vision Building
20 Greenmarket
Dundee
DD1 4QB

T: 01382 200055

Edinburgh

Ground Floor
11-15 Thistle Street
Edinburgh
EH2 1DF

T: 0131 226 0200

Glasgow

100 West George Street
Glasgow
G2 1PP

T: 0141 471 9870

mha HENDERSON LOGGIE

hlca.co.uk | info@hlca.co.uk

APPENDIX 3

Tayside Valuation Joint Board

Annual Report to the Joint Board and the Assessor on the Provision of Internal Audit Services for 2019/20

Internal Audit Report No: 2020/07

Draft issued: 21 July 2020

Final issued: 24 July 2020

Contents

	Page No.
1. Annual Report and Opinion	1 - 3
2. Reports Submitted	4 - 5
3. Summary of Results and Conclusions	6 - 11
4. Time Spent – Actual v Budget	12
5. Operational Plan for 2020/21	13

1. Annual Report and Opinion

Introduction

1.1 We were formally re-appointed in April 2019 as internal auditors of Tayside Valuation Joint Board ('the Board') for the period 1 April 2019 to 31 March 2022. This report summarises the internal audit work performed during 2019/20.

1.2 An Audit Needs Assessment (ANA), based on the areas of risk that the Board is exposed to, was prepared as part of our internal audit programme for 2019/20 (internal audit report 2020/01, issued in July 2019). The ANA was prepared following discussion with the Assessor, several senior Board personnel, the external auditors, and with reference to the CIPFA Code of Practice for Internal Audit in Local Government in the United Kingdom. The ANA was prepared on the basis of the normal three-year internal audit cycle, covering the period 2019/20 to 2021/22. Work in the previous three-year cycle was used to update the key control environment. Following on from the ANA, a Strategic Plan was formulated covering the three-year cycle.

1.3 The Internal Audit Annual Plan 2019/20 reflected the allocation of days shown in Year 1 of the Audit Needs Assessment and Strategic Plan 2019 to 2020, with no changes made.

1.4 The work delivered in 2019/20 followed that set out in the Annual Plan for 2019/20. The reports submitted are listed in Section 2 of this report and a summary of results and conclusions from each finalised assignment is given at Section 3.

1.5 An analysis of time spent against budget is shown below in Section 4.

Public Sector Internal Audit Standards (PSIAS) Reporting Requirements

1.6 The Board has responsibility for maintaining an effective internal audit activity. You have engaged us to provide an independent risk-based assurance and consultancy internal audit service. To help you assess that you are maintaining an effective internal audit activity we:

- Confirm our independence;
- Provide information about the year's activity and the work planned for next year in this report; and
- Provide quality assurance through self-assessment and independent external review of our methodology and operating practices.

1.7 Self-assessment is undertaken through:

- Our continuous improvement approach to our service. We will discuss any new developments with management throughout the year;
- Ensuring compliance with best professional practice, in particular the PSIAS;
- Annual confirmation from all staff that they comply with required ethical standards and remain independent of clients;
- Internal review of each assignment to confirm application of our methodology which is summarised in our internal audit manual; and
- Annual completion of a checklist to confirm PSIAS compliance. This is undertaken annually in April.

1.8 The results of our self-assessment are that we are able to confirm that our service is independent of the Board and complies with the PSIAS.

1.9 External assessment is built into our firm-wide quality assurance procedures. Henderson Loggie is a member of MHA, a national association of independent accountancy firms. Continued membership of MHA is dependent on maintaining a good level of quality and adhering to accounting and auditing standards in the provision of our services. Annual quality reviews are conducted to confirm our continuing achievement of this quality. The latest independent review in March 2019 included our internal audit service. Overall, the review found the firm's policies and procedures relating to internal audit to be compliant with the PSIAS.

Significant Issues

1.10 There were no significant issues or major internal control weaknesses noted from the internal audit work conducted during 2019/20. All internal audit reports issued during 2019/20 concluded that systems met control objectives and provided good assurance. A small number of actions have been agreed to further strengthen controls.

1.11 During 2019/20 the Board made progress in fully implementing three of the eight recommendations contained within internal audit reports issued in 2018/19. Our Follow-Up Reviews (Internal Audit Report 2020/06) reported that the remaining five recommendations were considered by management but not implemented, including:

- two recommendations raised in internal audit report 2019/04 – Maintenance of Accuracy of the Electoral Register – where, following further review, the system vendor confirmed that it would not be viable to incorporate the audit recommendations into the system; and
- three recommendations which were raised in reports in 2010/11 and 2014/15 relating to project management. As no opportunities have arisen, or are likely to arise in the foreseeable future, which would require a project management methodology to be applied it was agreed with the Assessor to remove these recommendations.

1.12 There were no instances of fraud identified from the audit work conducted during the year.

Opinion

1.13 As required by standard 2450 of PSIAS, the chief internal audit executive, is required to provide an annual report on the audit work carried out during the year and an opinion on the operation of controls within the Board. This opinion is used to inform the Board's annual governance statement. Within the Board this role currently resides with MHA Henderson Loggie based on the work that MHA Henderson Loggie have undertaken.

1.14 In our opinion, overall, the Board operates adequate internal control systems as defined in the Audit Needs Assessment. The audit and assurance work has not identified any significant gaps in the Board's control environment that would increase the risk of financial loss. This opinion has been arrived at taking into consideration the internal audit, risk management and other assurance work that has been undertaken during 2019/20 and in previous years since our original appointment in 2010.

2. Reports Submitted

Number	Title	Overall Grade	Recommendations	Priority 1	Priority 2	Priority 3
2020/01	ANA and Strategic Plan	**N/A**	N/A	N/A	N/A	N/A
2020/02	Annual Plan	**N/A**	N/A	N/A	N/A	N/A
2020/03	Performance Reporting	**Good**	-	-	-	-
2020/04	Staff Recruitment and Retention	**Satisfactory**	-	-	-	3
2020/05	IT Network Arrangements	**Satisfactory**	-	-	1	3
2020/06	Follow Up Reviews	**No recommendations required further action.**	-	-	-	-
2020/07	Annual Report	**N/A**	N/A	N/A	N/A	N/A

Overall gradings are defined as follows:

Good	System meets control objectives.
Satisfactory	System meets control objectives with some weaknesses present.
Requires improvement	System has weaknesses that could prevent it achieving control objectives.
Unacceptable	System cannot meet control objectives.

Action Grades

Priority 1	Issue subjecting the organisation to material risk and which requires to be brought to the attention of the Joint Board
Priority 2	Issue subjecting the organisation to significant risk and which should be addressed by the Assessor.
Priority 3	Matters subjecting the organisation to minor risk or which, if addressed, will enhance efficiency and effectiveness.

3. Summary of Results and Conclusions

2020/01 – Audit Needs Assessment and Strategic Plan 2019 to 2022

Final Issued – July 2019

A comprehensive ANA based on the areas of risk that the Board is exposed to was undertaken in July 2019. A Strategic Plan to cover the three-year internal audit cycle was then formulated (refer to paragraph 1.2 above).

2020/02 – Internal Audit Annual Plan 2019/20

Final Issued – July 2019

The purpose of this document was to present to the members of Tayside Valuation Joint Board ('the Board') the annual internal audit operating plan for the year ended 31 March 2020. The plan was based on the proposed allocation of audit days for 2019/20 set out in the Audit Needs Assessment and Strategic Plan 2019 to 2022. The preparation of the Strategic Plan involved dialogue with management and with the Treasurer (via the Assessor).

2020/03 – Performance Reporting

Final Issued – October 2019

The audit considered the format, content and timeliness of management information, both financial and non-financial, provided to senior management and to the Joint Board in terms of the Annual Public Performance Report. We also considered whether the information reported to the Joint Board is appropriate, and whether such information is accurate and easy to understand for those who use it.

Strengths

- Although the performance information needs of users have not been formally documented, we have concluded that the information provided is adequate to reasonably inform Board members and the public. This is based on our review of data reported to the Joint Board and published on the Board's website.
- Performance information is clearly set out, easily accessible, accurate and provided on a timely basis.
- Management information is available which: reports on appropriate key performance indicators; enables the impacts of key strategic objectives to be measured; allows income and costs to be analysed; and assists in forecasting; and
- Efficient processes are in place to produce and disseminate management information.

Weaknesses

- There were no significant weaknesses identified during our review.

The table below notes the objectives for this review and records the results:

Objective	Findings			
The objectives of our audit were to obtain reasonable assurance that:		**1**	**2**	**3**
1. The performance information needs of users have been identified and the information provided meets those needs.	**Good**	0	0	0
2. Performance information is clearly set out, easily accessible, accurate, provided on a timely basis and readily understood by users.	**Good**	0	0	0
3. Management information is available which: ◆ reports on appropriate key performance indicators and, where applicable, on outputs, outcomes and impacts; ◆ enables the impacts of key strategic and operational decisions to be measured; and ◆ allows income and costs and to be analysed at a more detailed level.	**Good**	0	0	0
4. Processes in place to provide and disseminate management information are efficient.	**Good**	0	0	0
		0	**0**	**0**
Overall Level of Assurance	**Good**	System meets control objectives		

2019/04 – Staff Recruitment and Retention / Organisational Development

Final Issued – December 2019

The scope of this audit was to consider whether the Board is making best use of its staff and included a high-level review of workforce planning; training; and succession planning.

The table below notes each separate objective for this review and records the results:

Objective	Findings			
The objectives of this audit were to obtain reasonable assurance that:		**1**	**2**	**3**
1. The Board has a systematic approach for ensuring that its staff resources match identified need in order to deliver planned commitments. Where gaps are identified, timely action is taken to close these.	**Satisfactory**	0	0	2
2. A systematic process is used for providing feedback to staff on performance and agreeing action to improve performance.	**Good**	0	0	0
3. The Board's approach to training, including induction training, is clearly informed by an assessment of where there are skills / knowledge / performance gaps.	**Good**	0	0	0
4. The Board has a systematic approach to evaluating its training to ensure that it is achieving the desired impact.	**Satisfactory**	0	0	1
5. Appropriate succession planning strategies, action plans and monitoring arrangements are in place.	**Good**	0	0	0
Overall Level of Assurance	**Satisfactory**	**0**	**0**	**3**
		System meets control objectives with some weaknesses present		

2019/05 – IT Network Arrangements / Cyber Security

Final Issued – July 2020

This audit included a review of the Board's current position regarding IT Security in order to advise on areas that should be addressed in line with the latest guidance produced by National Cyber Security Centre (NCSC), the UK Government's national technical authority for cyber security.

Strengths

- A risk management regime has been established, which includes identifying information / cyber security as key strategic risks and establishing an IT security policy set to mitigate those risks.
- A baseline security build for network infrastructure is in place.
- Hardware and software inventories have been created.
- Processes are in place for applying updates and patches to all devices connected to the IT network.
- The IT architecture protects the organisation's network through use of firewalls and segregation controls which prevent direct connections to untrusted external services and protects internal IP addresses.
- Management of user accounts is linked to the organisation's new staff starter, leaver and change of role procedures.
- Network hardware is protected by an antivirus solution, which automatically scans for malware.
- Whitelisting of removable media is in place and devices are scanned for malware when connected to networked equipment.
- The Board has achieved the Cyber Essentials certification which demonstrates a clear commitment to cyber risk management.
- The Board's network also connects to, and forms part of, the UK Government's Public Services Network (PNS). The PNS is responsible for overseeing and managing the PSN compliance process, ensuring that organisations that connect to the PNS are adequately secured. As part of this process the PNS undertakes an annual health check of the Board's network security.

Weaknesses

- It is good practice for an organisation to run automated vulnerability scanning tools against all networked devices regularly and remedy any identified vulnerabilities within an agreed time frame. We noted that the Board engages with a third-party to provide a vulnerability management service which provides scanning and triage reporting of vulnerabilities on a limited number of network devices only.
- As part of a layered approach to network security, where possible, the auto run function should be disabled on devices to prevent the automatic import of malicious code from any type of removable media. Equally, if removable media is introduced, the system should automatically scan it for malicious content. We note that although tools are in place which automatically scan removable media autorun has not been disabled.
- Our review identified that although IT staff demonstrated a strong awareness of information security risks, and the dangers of phishing and malware are communicated to staff, the organisation is not yet in a position to demonstrate that the same level of awareness exists amongst the wider staff as currently there is no structured programme of information security training provided to staff or any mechanism for testing the effectiveness of training provided.

2019/05 – IT Network Arrangements / Cyber Security (continued)

The table below notes each separate objective for this review and records the results:

his review and records the results:

Objective	Findings			
The specific objective of this audit was to:		**1**	**2**	**3**
1. Review the internal controls in place which ensure the security of the IT network, the configuration of key elements of ICT infrastructure which protect access to data, plus the policy and procedures giving guidance as to how security should be managed by both the IT department and users. This covered the following areas: • Information risk management. • Secure configuration of ICT equipment. • Network security. • Managing user privileges. • ICT user education and awareness. • Incident management (including disaster recovery). • Malware prevention. • Monitoring. • Removable media controls; and • Home and mobile working.	**Satisfactory**	0	1	1
Overall Level of Assurance	**Satisfactory**	**0**	**1**	**3**
		System meets control objectives with some weaknesses present		

2020/06 – Follow-Up Report

Final Issued – July 2020

We carried out a follow up review of recommendations made in the following internal audit reports issued during 2018/19:

2019/02 – Risk Management / Business Continuity Planning
2019/04 – Maintenance of Accuracy of the Electoral Register; and
2019/05 – Follow-Up Reviews.

Reports 2019/01, 2019/03 and 2019/06 did not contain an action plan and therefore no follow-up was required as part of this review. Report 2019/05 included four outstanding actions that required to be followed up again this year.

The Board has made progress in fully implementing three of the eight recommendations followed up as part of this review. The remaining five recommendations have been considered by management but not implemented, including:

- two recommendations raised in internal audit report 2019/04 – Maintenance of Accuracy of the Electoral Register – where, following further review, the system vendor confirmed that it would not be viable to incorporate the audit recommendations into the system; and
- three recommendations which were raised in reports in 2010/11 and 2014/15 relating to project management. As no opportunities have arisen, or are likely to arise in the foreseeable future, which would require a project management methodology to be applied it was agreed with the Assessor to remove these recommendations.

4. Time Spent – Actual v Budget

	Report number	Planned days	Actual days fee'd	Days to fee at July 2020	Days to spend / WIP	Variance
Reputation						
Performance Reporting	2020/3	3	3	-	-	-
Staffing Issues						
Staff Recruitment and Retention / Organisational Development	2020/4	4	4	-	-	-
Information and IT						
IT Network Arrangements / Cyber Security	2020/05	3	-	3	-	-
Other Audit Activities						
Follow-up	2020/06	1	-	1	-	-
Management & planning, attendance at Joint Board meetings & liaising with external audit	2020/02	2	1	1	-	-
ANA	2020/01	2	2	-	-	-
		_____	____	____	_____	_____
Total		15	10	5	-	-
		======	====	====	=====	======

5. Operational Plan for 2020/21

5.1 Following our re-appointment as internal auditors for the period from 1 April 2019 to 31 March 2022 we prepared an Audit Needs Assessment and Strategic Plan for 2016 to 2019 (internal audit report 2020/01, which was issued in July 2019).

5.2 An extract from the Strategic Plan, in relation to 2020/21 is shown below.

Proposed allocation of audit days for 2020/21:

	Category	Priority	Planned 20/21 Days
Reputation			
Compliance with Legislation	Gov	M / L	3
Non-Domestic Rates			
Maintenance of the Accuracy of Records Relating to Current Property Values / Valuation and Updating Procedures / Administering Appeals / Control of Input to the Valuation Roll	Perf/Fin	M	5
Organisational Issues			
Corporate Governance	Gov	M	4
Other Audit Activities			
Management & planning, attendance at Joint Board meetings & liaising with external audit			2
Follow-up reviews		Various	1
			____
Total			**15**
			====

Aberdeen

45 Queen's Road
Aberdeen
AB15 4ZN

T: 01224 322100

Dundee

The Vision Building
20 Greenmarket
Dundee
DD1 4QB

T: 01382 200055

Edinburgh

Ground Floor
11-15 Thistle Street
Edinburgh
EH2 1DF

T: 0131 226 0200

Glasgow

100 West George Street
Glasgow
G2 1PP

T: 0141 471 9870

mha HENDERSON LOGGIE

hlca.co.uk | info@hlca.co.uk

APPENDIX 4

Tayside Valuation Joint Board

Internal Audit Annual Plan 2020/21

Internal Audit Report 2021/01

Draft Issued: 21 July 2020

Final Issued:

Now, for tomorrow

mha HENDERSON LOGGIE

Contents

1. Introduction **1**

2. Strategic Plan 2019 to 2022 **2**

3. Outline Scope and Objectives **5**

- Compliance with Legislation 5
- Non-Domestic Rates 6
- Corporate Governance 7
- Follow-Up Reviews 8

1. Introduction

1.1 The purpose of this document is to present to the members of Tayside Valuation Joint Board ('the Board') the annual internal audit operating plan for the year ended 31 March 2021. The plan is based on the proposed allocation of audit days for 2020/21 set out in the Audit Needs Assessment and Strategic Plan 2019 to 2022. The preparation of the Strategic Plan involved dialogue with management and with the Treasurer (via the Assessor).

1.2 At Section 3 of this report we have set out the outline scope and objectives for each audit assignment to be undertaken during 2020/21, together with the proposed audit approach. These were arrived at following discussion with the Assessor.

1.3 Separate reports will be issued for each assignment. Recommendations are graded in each report to reflect the significance of the issues raised.

1.4 Our audit service complies with the Public Sector Internal Audit Standards (PSIAS).

2. Strategic Plan 2019 to 2022

Audit Area	Risk Register Ref.	Previous IA Coverage	2019/20 Days	2020/21 Days	2021/22 Days	Objective
Reputation						
Compliance with Legislation	1.1, 4.6, 5.1, 7.4	All years		3		To ensure that there are effective arrangements to review compliance with key legislation including The Data Protection Act 2018 and the Non-Domestic Rates (Scotland) Act 2020. Compliance with relevant legislation will also be considered where applicable on all audits.
Performance Reporting		2016/17 - Good	3			To ensure that the format, content and timeliness of management information, both financial and non-financial, provided to senior management and to the Joint Board, focusses on what is set out in the Annual Public Performance Report. We will also consider whether the information reported to the Joint Board is appropriate, and whether such information is accurate and easy to understand for those who use it.
Council Tax						
Maintenance of the Accuracy of Records Relating to Property Bandings / Valuation and Updating Procedures / Administering Proposals / Control of Input to the Valuation List	5.2	2018/19 - Good			4	To review the adequacy and effectiveness of the controls and procedures in place to ensure the accuracy of records relating to all domestic properties within the Board's area and that all property bandings are appropriate and only approved changes, new entries, deletions and amendments, proposals and appeals are made to the Valuation List.

Audit Area	Risk Register Ref.	Previous IA Coverage	2019/20 Days	2020/21 Days	2021/22 Days	Objective
Non-Domestic Rates						
Maintenance of the Accuracy of Records Relating to Current Property Values / Valuation and Updating Procedures / Administering Appeals / Control of Input to the Valuation Roll	5.2	2017/18 - Good		5		To review adequacy and effectiveness of the controls and procedures in place to ensure that the records relating to current property values are up to date and accurate, valuations and appeals are dealt with appropriately and timeously, and appropriate controls are in place over entries and amendments made to the Valuation Roll. We will also review the Board's preparations for revaluation of non-domestic properties in April 2022.
Electoral Register						
Maintenance of Accuracy of the Electoral Register	Section 6	2018/19 - Good			4	To review the adequacy and effectiveness of the controls and procedures in place to ensure that the Register of Electors published annually for the Angus and Perth & Kinross council areas are up-to-date and accurate.
Staffing Issues						
Staff recruitment and retention / staff development		N/A	4			To review the adequacy and effectiveness of policies and procedures for staff recruitment and selection and the processes in place that contribute to the retention and engagement of staff, and arrangements for succession planning.
Estates and Facilities						
Budgetary Control		2015/16 - Good			4	To review the processes and controls in place for budget setting and budgetary control within the Tayside Valuation Joint Board.

Audit Area	Risk Register Ref.	Previous IA Coverage	2019/20 Days	2020/21 Days	2021/22 Days	Objective
Organisational Issues						
Corporate Governance		2017/18 - Good		4		Cyclical check to undertake a high-level review of the corporate governance arrangements in place within the Board to ensure that the governance framework represents best practice as set out in the CIPFA code of practice issued in September 2016. We will also review the Scheme of Delegation and Standing Orders.
Information and IT						
IT Network Arrangements / Cyber Security		2014/15	3			To carry out a high-level review of certain key aspects of the IT systems in place within the organisation to identify any control weaknesses. This will include a review the Board's position with regard to IT Security in order to advise on areas that should be addressed in line with the latest guidance produced by the National Cyber Security Centre (NCSC), the UK Government's national technical authority for information and cyber security assurance.
Other Audit Activities						
Management & planning, attendance at Joint Board meetings & liaising with external audit			2	2	2	
Follow-up			1	1	1	Follow up of outstanding internal audit recommendations.
ANA			2	-	-	
Total			**15**	**15**	**15**	

3. Outline Scope and Objectives

Audit Assignment:	Compliance with Legislation
Priority:	Medium / Low
Joint Board Meeting:	June 2021
Days:	3

Scope

This audit will involve a high-level review of the processes in place within the organisation for the maintenance of policies and procedures and will consider the arrangements in place to ensure compliance with key legislation, including the Data Protection Act 2018 and the Non-Domestic Rates (Scotland) Act 2020.

Objectives of the Audit

The objective of our audit will be to obtain reasonable assurance that:

- there is a consistent approach in place for the creation, amendment, approval and distribution of policies and procedures;
- all policies and procedures are reviewed, and updated where necessary, on a periodic basis;
- outwith the normal review cycle there is a process to identify changes in legislation and update policies and procedures on a timely basis;
- policies and procedures in place cover all appropriate areas and are considered adequate; and
- staff have access to policies and procedures and are aware of their requirements.

Audit Approach

From discussion with the Assessor and Administration Manager we will establish the process in place for the creation, amendment, approval and distribution of policies and procedures and consider whether this is in line with good practice. We will also consider whether the policies and procedures in place cover all areas expected by legislation and good practice.

Audit Assignment:	Non-Domestic Rates
Priority:	Medium
Joint Board Meeting:	January 2021
Days:	5

Scope

This audit will review the adequacy and effectiveness of the controls and procedures in place to ensure that the records relating to current property values are up to date and accurate, valuations and appeals are dealt with appropriately and timeously, and appropriate controls are in place over entries and amendments made to the Valuation Roll. We will also review the Board's preparations for revaluation of non-domestic properties in April 2022.

Objectives

The specific objectives of the review will be to seek reasonable assurance that:

- there are appropriate procedures in place to ensure that: all non-domestic properties are on the Valuation Roll;
- all property valuations are carried out by suitably qualified valuers and are evidenced as checked and authorised by a Valuer or Senior Valuer;
- all valuations are input into the Valuation Roll and the weekly 'Roll of Change' is evidenced as checked by an Assistant Assessor or Principal Valuer;
- all appeal applications are logged on the appeals system as soon as they are received and are accepted and checked by a Valuer or Senior Valuer;
- the Valuation Roll is accurately and timeously amended to record the outcome of an appeal;
- only authorised staff can input amendments and all new entries are checked independently and evidenced;
- authorised staff change their passwords in line with pre-determined password protocols and where staff leave their access is suspended;
- all deletions are properly authorised by a Valuer or Senior Valuer and there are procedures in place to ensure that staff do not make alterations to any properties on the Roll in which they have an interest;
- a Valuation Notice is produced and sent out to the responsible party in line with legal requirements and any subsequent appeals are lodged within six months of the Valuation Notice being issued;
- preparations have been made, including an action plan and timescales, for the next revaluation of non-domestic properties which comes into force on 1 April 2022.

Audit Approach

From discussion with relevant staff, and review of procedural documentation, we will confirm any system changes, identify the key internal controls in place within the non-domestic rates valuation and appeals systems and compare these with expected controls. Audit testing will then be carried out to ensure that the controls in place are operating effectively across each area office.

Audit Assignment:	Corporate Governance
Priority:	Medium
Joint Board Meeting:	November 2020
Days:	4

Scope

This review will cover corporate governance arrangements within the Board and compare these against best practice included in the CIPFA Delivering Good Governance in Local Government: Guidance Note for Scottish Authorities (2016). This includes reviewing such items as:

- Code of Corporate Governance;
- Committee organisation and administration;
- Standing Orders;
- Financial Regulations;
- Delegation of Powers to Officers;
- Governance self-assessments;
- Fraud and Corruption policies and procedures;
- Complaints and Whistleblowing procedures.

Objectives

The primary objective of the audit will be to obtain reasonable assurance that the Board's corporate governance arrangements are in accordance with best practice as set out in the CIPFA / SOLACE Delivering Good Governance in Local Government: Framework (2016) and accompanying guidance notes for Scottish Authorities, which was published in September 2016.

Our audit approach will be:

We will identify the corporate governance arrangements in place through interviews with the Assessor and other relevant staff, and analysis of any corporate governance self-assessment. Relevant supporting documentation will also be reviewed to gain evidence that the arrangements in place have been adequately documented, communicated and are operating effectively.

Audit Assignment:	Follow-Up Reviews
Priority:	Various
Joint Board Meeting:	June 2021
Days:	1

Scope

This review will cover the following reports from the 2019/20 internal audit programme and reports from earlier years where previous follow-up identified recommendations outstanding:

- Report 2020/04 – Staff Recruitment and Retention / Organisational Development;
- Report 2020/05 – IT Network Arrangements / Cyber Security; and
- Report 2020/06 – Follow-up Reviews.

Internal Audit Reports 2020/01 – Audit Needs Assessment and Strategic Plan 2019 to 2022; 2020/02 – Annual Plan 2019/20, 2020/03 – Performance Reporting and 2020/07 – Annual Report 2019/20 did not contain any action plans and therefore no follow-up of these reports is required.

Objective

The objective of our follow-up review will be to assess whether recommendations made in internal audit reports from 2019/20 (and outstanding actions from previous years) have been appropriately implemented and to ensure that where little or no progress has been made towards implementation, that plans are in place to progress them.

Our audit approach will be:

- to request from responsible officers for each report listed above an update on the status of implementation of the recommendations made;
- to ascertain by review of supporting documentation, for any significant recommendations within the reports listed above, whether action undertaken has been adequate; and
- prepare a summary of the current status of the recommendations for the Board.

Aberdeen

45 Queen's Road
Aberdeen
AB15 4ZN

T: 01224 322100

Dundee

The Vision Building
20 Greenmarket
Dundee
DD1 4QB

T: 01382 200055

Edinburgh

Ground Floor
11-15 Thistle Street
Edinburgh
EH2 1DF

T: 0131 226 0200

Glasgow

100 West George Street
Glasgow
G2 1PP

T: 0141 471 9870

mha HENDERSON LOGGIE

hlca.co.uk | info@hlca.co.uk