

Lothian Valuation Joint Board

Internal Audit – Annual Opinion 2017/2018

3rd September 2018

1 Purpose of report

- 1.1 This report details Internal Audit's annual opinion for the Lothian Valuation Joint Board (LVJB) for the year ended 31 March 2018. Our opinion is based on the outcomes of the audits included in the 2017/18 Internal Audit annual plan; the status of any open Internal Audit findings; and review of the LVJB draft annual governance statement.

2 Main Report

Background

- 2.1 The objective of Internal Audit is to provide a high quality independent audit service to LVJB in accordance with Public Sector Internal Audit Standards (PSIAS) requirements, that provides assurance over the control environment established to manage LVJB's key risks and their overall governance and risk management arrangements.
- 2.2 PSIAS provide a coherent and consistent internal audit framework for public sector organisations. Adoption of the PSIAS is mandatory for internal audit teams within UK public sector organisations, and PSIAS require annual reporting on conformance.
- 2.3 It is the responsibility of the Council's Chief Internal Auditor to provide an independent and objective annual opinion on the adequacy and effectiveness of the LVJB control environment and governance and risk management frameworks in line with PSIAS requirements. The opinion is provided to the LVJB Board, and should be used to inform the LVJB annual governance statement.
- 2.4 The City of Edinburgh Internal Audit team currently performs one annual audit that focuses on the key controls established to manage LVJB's most significant risks.
- 2.5 The annual opinion provides an independent view of the adequacy and effectiveness of the LVJB control environment and governance and risk management frameworks, and is based on the outcomes of the audit(s) performed; the status of any open Internal Audit findings; and review of the LVJB draft annual governance statement.
- 2.6 Where control weaknesses are identified, Internal Audit findings are raised, and management agree actions to address the gaps identified. However, it is the responsibility of management to address and rectify the weaknesses identified via timely implementation of these agreed management actions.
- 2.7 The IA definition of an overdue finding is any finding where all agreed management actions have not been implemented by the final date agreed by management and recorded in Internal Audit reports.

Basis of opinion

- 2.8 Internal Audit days allocated to LVJB in the year to 31 March 2018 were split into two separate reviews. Our opinion is based on the outcome of these two audits; the status of

any open internal audit findings; and review of the LVJB draft annual governance statement.

Audit outcomes – Review of Data and Records Management Framework

- 2.9 This audit assessed the design adequacy of the established LVJB data and records management framework across the three lines of defence, by considering whether a total of 54 expected controls had been established and were adequately designed.
- 2.10 Our review confirmed that the LVJB data and records management framework is generally adequate, with enhancements required. This assessment is based on the outcomes of our review; the fact that LVJB has not suffered any recent significant data breaches or losses; and management's awareness of the control gaps identified.
- 2.11 There were 3 expected controls (5%) that had not been implemented or were partially implemented, where LVJB could be exposed to significant levels of risk.
- 2.12 These reflected the need to implement testing to assess levels of employee cyber security awareness as per the requirements of the Scottish Government Public Sector Action Plan for Cyber Resiliency; address use of generic usernames and password sharing for system administrator accounts; and implement appropriate data sharing arrangements with all key third parties.
- 2.13 A further 19 expected controls (35%) were not implemented or had been partially implemented, that could expose LVJB to moderate risk; with 32 expected controls (60%) established and adequately designed.

Audit outcomes – Review of Business Rates Internal Assurance Framework

- 2.14 This audit focused on the adequacy of design of LVJB's internal business rates valuation internal assurance framework.
- 2.15 Our review confirmed that the business rates internal assurance framework is generally adequate, with enhancements required. This assessment is based on the outcomes of our review; the fact that there have been no significant issues identified with the completeness and accuracy of source business rates valuation data; and no significant valuations errors.
- 2.16 We raised a total of 10 findings (8 medium and 2 low) highlighting the need to improve the internal business rates valuation assurance framework to mitigate exposure to moderate levels of risk. Addressing these findings will ensure that first and second line assurance over the operational and system controls supporting maintenance of the valuation roll and valuations calculations is strengthened.

Status of Internal Audit Findings

- 2.17 All Internal Audit findings raised in 2015/16 and 2016/17 have been addressed and agreed management actions effectively implemented and sustained.

Review of LVJB draft annual governance statement schedule

- 2.18 Review of the schedule prepared by management supporting the LVJB annual governance statement did not identify any instances of non-compliance highlighted in the management responses that would adversely impact on our internal audit opinion.

Internal Audit Independence

- 2.19 PSIAS require that Internal Audit must be independent and internal auditors must be objective in performing their work. To ensure conformance with these requirements, Internal Audit has established processes to ensure that both team and personal independence is consistently maintained and that any potential conflicts of interest are effectively managed.

- 2.20 We do not consider that we have faced any significant threats to our independence during 2017/18, nor do we consider that we have faced any inappropriate scope or resource limitations when completing our work.

Conformance with Public Sector Internal Audit Standards

- 2.21 Internal Audit has not conformed with PSIAS requirements during 2017/18 for the following reasons:
- 2.21.1 There has been insufficient follow-up of Internal Audit findings between April 2015 and October 2017 to monitor and ensure that management actions have been effectively implemented (PSIAS 2500); and
 - 2.21.2 Resourcing challenges within the Internal Audit team has impacted completion of the two internal quality assurance reviews included in the 2017/18 Internal Audit annual plan to ensure consistency of audit quality (PSIAS 1300).
- 2.22 It should be noted that these instances of non-conformance have had no direct impact on the quality of internal audit reviews completed for LVJB in 2017/18.

3 Conclusions

Internal Audit Annual Opinion

- 3.1 Internal Audit considers that the LVJB control environment and governance and risk management frameworks are generally adequate, but with enhancements required, and is therefore reporting an 'amber' rated opinion (see Appendix 1), with our assessment towards the low end of this category.
- 3.2 This opinion is subject to the inherent limitations of internal audit (covering both the control environment and the assurance provided over controls) as set out in Appendix 2.
- 3.3 This report is a component part of the overall annual assurance provided to LVJB, and the Board should consider the opinion of other assurance sources (such as external audit) when forming their own view on the design and effectiveness of the control environment and governance and risk management frameworks at LVJB.

4 Recommendations

- 4.1 The Board is recommended to note the internal audit opinion for the year ended 31 March 2018.

Lesley Newdall,
Chief Internal Auditor
City of Edinburgh Council

Appendices:	Appendix 1	Internal Audit Annual Opinion Definitions
	Appendix 2	Limitations and responsibilities of internal audit and management responsibilities
	Appendix 3	Final Internal Audit report – Review of Data and Records Management Framework
	Appendix 4	Final Internal Audit report – Review of Business Rates Internal Assurance Framework

Contact/Tel: E-mail: lesley.newdall@edinburgh.gov.uk | Tel: 0131 469 3216

Background Papers: [Public Sector Internal Audit Standards](#)

Appendix 1 – Internal Audit Annual Opinion Definitions

The PSIAS require the provision of an annual Internal Audit opinion, but do not provide any methodology or guidance detailing how the opinion should be defined. We have adopted the approach set out below to form an opinion for Lothian Pension Fund.

We consider that there are 4 possible opinion types that could apply to LVJB. These are detailed below:

1 Adequate <i>An adequate and appropriate control environment and governance and risk management framework is in place enabling the risks to achieving organisation objectives to be managed</i>	2 Generally adequate but with enhancements required <i>Areas of weakness and non-compliance in the control environment and governance and risk management framework that may put the achievement of organisational objectives at risk</i>
3 Significant enhancements required <i>Significant areas of weakness and non-compliance in the control environment and governance and risk management framework that puts the achievement of organisational objectives at risk</i>	Inadequate <i>The framework of control and governance and risk management framework is inadequate with a substantial risk of system failure resulting in the likely failure to achieve organisational objectives.</i>

Professional judgement is exercised in determining the appropriate opinion, and it should be noted that in giving an opinion, assurance provided can never be absolute.

Appendix 2 - Limitations and responsibilities of internal audit and management responsibilities

Limitations and responsibilities of internal audit

The opinion is based solely on the internal audit work performed for the financial year 1 April 2017 to 31 March 2018. Work completed was based on the terms of reference agreed with management. However, where other matters have come to our attention that are considered relevant, they have been considered when finalising our reports and the annual opinion.

There may be additional weaknesses in the LVJB control environment and governance and risk management frameworks that were not identified as they were not included in the 2017/18 audit review; were excluded from the scope of the review; or were not brought to Internal Audit's attention. Consequently, management and the Board should be aware that the opinion may have differed if these areas had been included, or brought to Internal Audit's attention.

Control environments, no matter how well designed and operated, are affected by inherent limitations. These include the possibility of poor judgment in decision-making; human error; control processes being deliberately circumvented by employees and others; management overriding controls; and the impact of unplanned events.

Future periods

The assessment of controls relating to LVJB is for the year ended 31 March 2017. Historic evaluation of effectiveness may not be relevant to future periods due to the risk that:

- the design of controls may become inadequate because of changes in operating environment, law, regulation or other; or
- the degree of compliance with policies and procedures may deteriorate.

Responsibilities of Management and Internal Audit

It is Management's responsibility to develop and effective control environments and governance and risk management frameworks that are designed to prevent and detect irregularities and fraud. Internal audit work should not be regarded as a substitute for Management's responsibilities for the design and operation of these controls.

Internal Audit endeavours to plan its work so that it has a reasonable expectation of detecting significant control weaknesses and, if detected, performs additional work directed towards identification of potential fraud or other irregularities. However, internal audit procedures alone, even when performed with due professional care, do not guarantee that fraud will be detected.

Consequently, internal audit reviews should not be relied upon to detect and disclose all fraud, defalcations or other irregularities that may exist.

Lothian Valuation Joint Board

Internal Audit Report

Review of Data and Records Management Framework

27 August 2018

LVJB1701

Contents

1. Background and Scope	1
2. Executive summary	3
3. Detailed findings	5
Appendix 1 - Basis of our classifications	24
Appendix 2 – Terms of Reference	25

This Internal Audit review is undertaken as part of the established service level agreement with the Lothian Valuation Joint Board that covers provision of Internal Audit services by the City of Edinburgh Council.

The review is designed to help the Lothian Valuation Joint Board assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose or by any other party.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Whilst a number of specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud.

This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate.

1. Background and Scope

Background

The Lothian Valuation Joint Board (LVJB) is a statutory entity established under the 1995 Valuation Joint Boards Order. LVJB provides a range of specialist valuation and electoral registration services for the Edinburgh; East Lothian; West Lothian; and Mid Lothian local authorities, and is responsible for the management and ongoing administration of their Business Rates Valuation Rolls; Council Tax Valuation Lists; and Electoral Registers.

Given the financial, fiscal, and democratic importance of these rolls and registers to the local authorities, it is essential that LVJB has an established data and records management framework which is appropriately designed and operates effectively to ensure that data and records are completely and accurately processed; and managed in line with current Data Protection Act requirements.

On 25 May 2018, the new European Union (EU) General Data Protection Regulations (GDPR) will become effective in the UK. Achieving full compliance with the new regulations is an evolving process as the legislation and supporting GDPR guidance has not been fully finalised. As a minimum, organisations are expected to have performed a gap analysis against the new legislative requirements; identified any specific control gaps; and developed an implementation plan to address the gaps identified by 25th May 2018.

Adequate and effective cyber security controls are also key to ensuring that data and records are effectively protected. LVJB will also need to ensure that their cyber security controls meet the requirements of the [Scottish Government Public Sector Action Plan for Cyber Resilience](#) published in November 2017.

In 2014/15 LVJB obtained accreditation to use the Public Services Network (PSN), the UK Government's secure high-performance network which helps public sector organisations work together, reduce duplication and share resources safely and securely. Ongoing accreditation requires LVJB to demonstrate compliance with a range of technology security requirements prescribed by the Cabinet Office. These include completion of an annual Network Penetration Test and an IT Security Health check performed by an independent accredited third-party provider; and submission of an annual compliance confirmation to the Cabinet Office. PSN accreditation provides additional assurance that data and records are managed securely.

Records management frameworks can also be considered in the context of the three lines of defence model where the first line is those employees responsible for applying controls when processing and managing data; the second line is those responsible for defining records management frameworks and policies, and assessing ongoing compliance with them; with the independent third line responsible for providing assurance that the framework is appropriately designed and operating effectively.

Scope

Our review was performed as at **31 March 2018**, and focused on the adequacy of design of the LVJB data and records management framework across the three lines of defence.

We assessed whether a total of 54 expected data and records management controls had been established and were adequately designed across the following areas:

1. Data and records management governance framework
2. Training and awareness
3. Data assets and flows
4. Data retention and destruction
5. Data access and security
6. Subject access and freedom of information requests

7. Third party data sharing arrangements
8. Data breaches
9. GDPR readiness
10. Business change projects

Scope Limitations

The following areas were specifically excluded from the scope of our review:

- Assessment of the effectiveness of the controls supporting the data and records management framework; and
- Ongoing Public Sector Network compliance requirements.

2. Executive Summary

Overall Assessment




Our review confirmed that the LVJB data and records management framework is generally adequate, with enhancements required. This assessment is based on the outcomes of our review; the fact that LVJB has not suffered any recent significant data breaches or losses; and management's awareness of the control gaps identified.

The outcomes of our review are summarised in the table below, and confirm that some control gaps exist in the data and records management framework. Notably, there were 3 expected controls (5%) that had not been implemented, or had been partially implemented, where LVJB could be exposed to significant levels of risk; with a further 19 (35%) that could result in moderate exposure to risk.

A total of 32 expected controls (60%) had been established and were adequately designed, with low exposure to risk.




It is important that these significant and moderate control gaps are addressed by management in a timely manner to ensure that the LVJB data and records management framework is appropriately designed to protect the data that they obtain; process; retain; and share with others, and meets the new GDPR and Public Sector Action Plan for Cyber Resiliency requirements.

Summary of findings

#	Area covered	Low Risk 	Moderate Risk 	High Risk 	Total
1	Data and records management governance framework	3	5	-	8
2	Training and awareness	4	2	1	7
3	Data assets and flows	2	2	-	4
4	Data retention and destruction	2	2	-	4
5	Data access and security	11	6	1	18
6	Subject access and freedom of information requests	5	-	-	5
7	Third party data sharing arrangements	-	-	1	1
8	Data breaches	-	2	-	2

9	GDPR readiness	3	-	-	3
10	Business change projects	2	-	-	2
Totals		32	19	3	54

Key

-  Controls established and well designed with Low exposure to risk;
-  Some control design gaps evident with Moderate risk exposure if not addressed; and
-  Significant control gaps evident with High Risk exposure if not addressed.

High Risk Control Gaps

The control gaps we identified that could potentially result in exposure to high levels of risk are:

- Cyber Security Training and Awareness (finding 2.6 - partially implemented)** – currently, very limited testing is performed to assess levels of employee cyber security knowledge (for example, simulated phishing exercises). If employees lack knowledge, there is a risk that they click on attachments or spoof or hoax web page links included in phishing e mails, resulting in installation of malware or ransomware across the LVJB network.

Additionally, per the requirements of the Public Sector Action Plan for Cyber Resiliency, the Scottish Government will seek assurances from Scottish public bodies that they have established appropriate staff training, awareness-raising and disciplinary processes with regard to cyber resilience for staff at all organisational levels (key action 6); and that they have obtained appropriate independent assurance on their critical cyber security controls by October 2018 (key action 4);
- Data Access and Security (finding 5.5 - not implemented)** - management has advised that there are some system administrator accounts where generic user names and complex passwords are shared by more than one senior officer; and
- Third party data sharing arrangements (finding 7.1 - partially implemented)** - data sharing arrangements have not been established with all key third parties to ensure that data is consistently transferred; shared; and stored securely.

The detailed outcomes of our review, including agreed management actions and implementation timeframes are included at section 3 [Detailed Findings](#) below.




Finally, it is recommended that progress with implementation of the High and Moderated rated actions are monitored via the new Governance Committee, with regular updates provided to the Board.



Internal audit will also review the full population of the High and a sample of the moderate rated actions as part of the 2019/20 LVJB review to confirm that they have been effectively implemented and sustained.

3. Detailed Findings

Key

Control Established: Y- Yes; P – Partially; and N – No

-  Controls established and well designed with Low exposure to risk;
-  Some control design gaps evident with Moderate risk exposure if not addressed; and
-  Significant control gaps evident with High Risk exposure if not addressed.

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
1. Data and Records Management Governance Framework							
1.1	Responsibility for data and records management framework has been allocated at an appropriate level (Second Line)				The Governance Manager has responsibility for the data and records management framework, and reports to the Principal Assessor as Chief Accountable Officer and ultimately to the LVJB Board.	N/A	N/A
1.2	An appropriate governance committee is responsible for oversight of the data and records management framework. (Second Line)				<p>The LVJB Board has ultimate responsibility for oversight, but has had only limited coverage of data and records management in recent years.</p> <p>A new governance committee is being established (May 2018) that will include data and records management as part of its remit.</p> <p>The responsibilities and composition of the new committee is still being decided, but consideration should be given to ensuring Board member inclusion as well as input from specialists (Internal Audit / IT Risk Auditors etc.) as and when required.</p>	<p>1.2.1 Establish remit, scope, membership, and structure of new 'Governance' Committee.</p> <p>1.2.2 Incorporate Board members and (where appropriate) external specialist input into the structure / membership of the new 'Governance' Committee. (1.2)</p>	<p>Creation of the new "internal facing" Governance group will be established by the end of May 2018.</p> <p>The incorporation of Board members and other external parties shall be discussed and consulted upon with a view to adoption by the end of 2018.</p> <p>Owner: Bernie Callaghan, Governance Manager</p> <p>Date: 29 June 2018</p>

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
1.3	Policy and procedure documents are in place covering all aspects of data and records management; data processing; and data protection. (Second Line)		⊙		LVJB has an established and comprehensive Information and Technology Management Security Policy (ITMS Policy). This includes data and records management; data protection; and data security. However, some gaps in the content of the ITMS policy have been identified in relation to inclusion of the processes to be applied when working at home via the virtual private network (VPN) and the process to be applied in the event of a significant data breach or loss. These are covered in more detail at 5.15 and 8.1 below.	N/A	N/A
1.4	Policy and procedure documents are reviewed and updated on a regular basis. (Second Line)	⊙			The ITMS Policy is reviewed and revised annually. The last update was June 2017.	N/A	N/A
1.5	Data and records management, data processing and data protection risks are appropriately considered in the organisational risk register. (Second Line)		⊙		Data and records management and associated IT security risks are reflected in the corporate risk register. However, there is an opportunity to revise the risk register to reflect current and emerging risks as some of the content is of date. Given the significance of cyber, data and IT security risks, many organisations now maintain a supplementary 'technology and data risk' register to ensure appropriate focus on new and emerging risks and appropriate controls.	1.5.1 Update and refresh the technology and data risk aspects of the current corporate risk register. 1.5.2 Establish a more detailed and comprehensive 'technology and data risk register' to record new and emerging risks and the controls in place to manage them.	1.5.1 A review and update of the corporate risk register will be complete by June 2018. Owner: Bernie Callaghan, Governance Manager Date: 29 June 2018 1.5.2 Consideration of the creation of a "technology and data risk" register will also be completed by Autumn 2018.

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
							Owner: Bernie Callaghan, Governance Manager Date: 1 October 2018
1.6	There is regular management and Board / Committee reporting on data and records management. (Second Line)		⊙		<p>Data and records management is reported throughout the organisation (for example, to Senior Management; the IT Group; and Records Management Group).</p> <p>However, there is no formal reporting on data and records management at Board level although key messages would be communicated as required.</p> <p>The new governance committee referred to at 1.2 above will ensure more detailed and specific focus and reporting on data and records management going forward.</p>	<p>1.6.1 Establish more regular (for example quarterly or six monthly) and structured reporting (based on key performance indicators) on data and records management at Board / Committee.</p> <p>Also refer section 6 below in relation to reporting on volumes of subject access and freedom of information requests received and processed.</p>	<p>1.6.1 Summary reporting of technology/data risks will be incorporated into existing reporting procedures at Board level by the end of 2018.</p> <p>Owner: Bernie Callaghan, Governance Manager Date: 1 December 2018</p>
1.7	Relevant measurable key performance indicators have been established to support reporting on data management, data processing and data / information security. (Second Line)		⊙		<p>As noted at 1.6 above, there is an opportunity for more formal reporting in these areas.</p> <p>Management has advised the data required to prepare information for Board and governance committee reporting is available, but not consolidated into formal governance reports, and that no key performance indicators have been established.</p>	<p>1.7.1 Ensure reporting includes relevant statistics and KPIs, such as:</p> <ul style="list-style-type: none"> • Volumes of, and trends in data processed; • Data protection and security incidents and near misses; • Subject Access and Freedom of Information Requests; • Attacks filtered / stopped by firewall; Phishing incidents intercepted; and 	<p>1.7.1 Subject Access and FOI Requests are already presented at Corporate Leadership Meetings and Governance Committee. As mentioned above technology/data risk reporting will be reported on later in the year.</p> <p>Owner: Bernie Callaghan, Governance Manager Date: 1 December 2018</p>

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
						<ul style="list-style-type: none"> Unusual or exceptional network traffic. 	
1.8	Independent assurance is provided on the design and effectiveness of the data and records management framework. (Third Line)	⊙			<p>Could be covered by the scope of the annual audit performed by City of Edinburgh Council.</p> <p>An annual network penetration test and an IT security health check is performed by an accredited third-party provider to support submission of an annual public sector network compliance confirmation to the Cabinet Office.</p>	N/A	N/A
2. Training and Awareness							
2.1	Data and records management is included in the new employee induction process. (First Line)	⊙			New employee induction training includes an overview of LVJB policies and procedures and completion of a short online e-learning module, which both cover data and records management.	N/A	N/A
2.2	Annual data and records management training is provided to and completed by all employees and Board members. (First Line)			⊙	<p>All new employees and administrative employees have data and records management training via completion of an e-learning module.</p> <p>No specific training has been provided for technical staff.</p> <p>No specific training has been provided for Board members.</p>	<p>2.2.1 Ensure LVJB technical staff complete the relevant data and record management training;</p> <p>2.2.2 Consider whether data and records management training should be provided for Board members; and</p> <p>2.2.3 If provided, training should focus on General Data Protection Regulation requirements; the risks associated with data and</p>	<p>Complete: GDPR training has been rolled out to all staff. Annual refresher training will be introduced as we move forward.</p> <p>2.2.2 Data and records management training should be provided to Board members by their parent authority.</p>

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
						records management; and the controls applied by LVJB.	
2.3	Policy and procedure documents are appropriately communicated to and acknowledged by all employees, and evidence retained. (Second Line)	⊙			New employees receive an overview of LVJB policies and procedures as part of their induction training, and sign a confirmation slip. The Head of Governance is keen to establish a more specific sign off from all employees confirming their understanding of requirements of the ITMS policy. Evidence of employee completion of the e-learning module is retained by the Secretariat team.	2.3.1 Establish a specific annual sign-off from all employees to confirm their understanding of the ITMS policy.	2.3.1 All new and reviewed policies must be "signed off" via email response from staff. The emails are retained by the Governance team as evidence of this. Owner: Bernie Callaghan, Governance Manager Date: 1 May 2018
2.4	Specific data and records management and data protection training has been provided (where appropriate) to employees in higher risk roles. (First Line)		⊙		IT team members have been supported through an additional technical qualification. The Governance Manager has attended several specific events and training sessions in relation to GDPR. Senior Managers and above have also received an internal GDPR briefing. Whilst a general training plan is in place, management recognise that a more structured and strategic training plan is required in relation to data processing; records management and information security risks.	2.4.1 A structured training plan / awareness strategy should be developed and implemented, with training delivered to all relevant employees.	2.4.1 This will be introduced by the end of 2018, consideration will also be given to risk management training/awareness for Board members of the Governance committee by this date. Owner: Bernie Callaghan, Governance Manager Date: 1 December 2018

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
2.5	There is an ongoing programme of general data risk awareness within the organisation. (First Line)	⊙			Ongoing awareness is maintained via intranet content and awareness posters on noticeboards etc.	N/A	N/A
2.6	Simulated 'phishing' exercises are undertaken to assess the organisation's awareness and sensitivity to data risk. (Second Line)		⊙		<p>No simulated email phishing exercises have yet been performed, however, internal testing was performed where USB devices were left in the canteen area to observe reactions and responses.</p> <p>The Public Sector Action Plan for Cyber Resiliency (key action 6) The Scottish Government will seek assurances from Scottish public bodies that they have in place appropriate staff training, awareness-raising and disciplinary processes with regard to cyber resilience for staff at all organisational levels</p> <p>Key action 4 also requires the public sector organisations to obtain appropriate independent assurance of critical cyber security controls by end October 2018</p> <p>A network penetration test is also by an accredited third-party provider to support ongoing public sector network accreditation.</p>	<p>2.6.1 Consider performing a simulated 'phishing' exercise to assess levels of employee risk awareness and effectiveness cyber security controls by October 2018.</p> <p>2.6.2 Once completed, action plans should be established to address any weaknesses identified.</p>	<p>2.6.1 A simulated 'phishing' exercise will be undertaken by July 2018.</p> <p>2.6.2 Action Plans shall be developed following the exercise.</p> <p>Owner: Bernie Callaghan, Governance Manager Date: 1 September 2018</p>
2.7	Weaknesses identified from phishing simulation exercises	⊙			Management has advised that no significant weaknesses have been	N/A	N/A

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
	or network penetration testing have been addressed. (Second Line)				identified from penetration testing performed.		
3 Data Assets and Flows							
3.1	There is a clear, detailed, and comprehensive record of the data assets, databases and data records held by the organisation (in both soft and hard copy) which includes identifies personal, sensitive data. (First Line)	⊙			There is a detailed Data Retention and Disposal Register which specifies all key data assets; data records; and transaction record types. Roles and responsibilities for ownership; retention; and deletion of data are also clearly defined. A detailed Personal Data Audit Template has also been completed (in preparation for GDPR compliance) that outlines the data assets, applications and databases held by LVJB. This includes information on the data held, what it is used for and who it is shared with (where relevant).	N/A	N/A
3.2	There is a clearly identified individual with ownership for individual data assets, databases and records held (soft and hard copy). (First Line)	⊙			This is included as part of the Data Retention and Disposal Register described at 3.1 above.	N/A	N/A
3.3	The flow of data within and outside the organisation has been recorded, mapped, and documented – with specific focus on personal sensitive data.		⊙		The Personal Data Audit Template (spreadsheet) provides an overview of personal data sets and outlines which third parties personal data is shared with (where relevant).	3.3.1 Management should assess whether further and more detailed data mapping is required or whether the current higher level 'data structure	3.3.1 Due to the nature of this task it will be considered by the Project Management Board by the end of 2018 before a

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
	(First Line)				Some elements of data and records management processes have been mapped in detail, however these process maps do not cover the full population of organisational data flows.	mapping' already in place is sufficient to ensure GDPR compliance and highlight key data and records management risks.	decision is taken to undertake further work.
3.4	Data flow documentation is regularly reviewed and refreshed to ensure it remains accurate. (First Line)		⦿		The Personal Data Audit Template (spreadsheet) is subject to regular review, however, the Governance Manager has highlighted that further work is required to extend and refine the document.	3.4.1 Undertake further work to extend and refine the Personal Data Audit template that will be used to demonstrate GDPR compliance.	3.4.1 Complete. Further work has now taken place and the template is complete for GDPR purposes.
4 Data Retention and Destruction							
4.1	Data retention and disposal schedules are in place for all applicable data sets across the organisation. (First Line)	⦿			There is a detailed Data Retention and Disposal Register which outlines all key data record sets and transaction record types and specifies responsibilities for ownership, retention and deletion of data.	N/A	N/A
4.2	Data is archived and destroyed in line with established retention schedules. (First Line)			⦿	Management has advised that further work is required to confirm whether data is archived and destroyed in line with retention schedules.	4.2.1 A review should be performed to confirm whether data is archived and destroyed in line with retention schedules.	4.2.1 Work continues on bringing the existing LVJB Retention Management disposal schedule into force. Introduction of the GDPR should assist in this process by identifying designated Information Asset Owners and assigning implementation responsibility to the Chief

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
							Assessor as Senior Information Risk Owner. July 2018 Owner: Bernie Callaghan Date: 1 September 2018
4.3	Destruction of paper files is managed securely using secure confidential waste bins, with the contents subsequently destroyed by a certified supplier, minimising the risk of data leakage or breach. (First Line)			⦿	Paper files for destruction are disposed of into confidential waste paper sacks which are situated around the LVJB office. The paper is then shredded on site and uplifted by a certified supplier for final destruction.	4.3.1 Use of open sacks and on-site handling is not in line with good practice. Current arrangements should be replaced with secure confidential waste bins.	4.3.1 Revised arrangements will be implemented by June 2018. Owner: Bernie Callaghan Date: 29 June 2018
4.4	Disposal or destruction of IT equipment is performed securely using an accredited supplier to minimise the risk of data leakage or breach. (First Line)	⦿			LVJB aims to ensure that all data is held on the network and not is on mobile or peripheral devices. Any IT equipment to be disposed of is cleared of data internally by the IT team before being uplifted by a certified supplier. IT equipment awaiting uplift is stored in a separate meeting room (Salisbury Room) – management consider the risk of inappropriate access to this room to be low.	N/A	N/A

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
5 Data Access and Security							
5.1	Access to LVJB premises is appropriately controlled and restricted. (First Line)	⊙			Access to LVJB premises is secured through security fob access with visitors reporting to reception. Security fobs are issued by the Secretariat team and a log is maintained of all fobs issued and returned.	N/A	N/A
5.2	Access to LVJB hard copy data and records is appropriately controlled and restricted. (First Line)	⊙			Hard copy data and records are held in lockable file stores and cupboards. The Support Services team ensure that National Insurance and Date of Birth information is not left on desks or open access areas.	N/A	N/A
5.3	A clean desk policy is in place and consistently applied at LVJB premises. (First Line)		⦿		A clean desk policy is in place but is not always observed or enforced. Clean desk sweeps and checks are not regularly performed.	5.3.1 Regular clean desk checks should be performed on an ongoing basis, with any personal data identified during the exercise appropriately secured, and feedback provided to the relevant team / employees.	5.3.1 The process of enforcement will commence from July 2018. Owner: Bernie Callaghan Date: 31 July 2018
5.4	Access to electronic data (IT systems, applications, data sets etc.) is appropriately restricted to relevant authorised employees. (First Line)	⊙			Access to the LVJB network and key applications is subject to username and password authentication controls. Access and permission rights within key applications (such as CVS) is tiered based on user roles and seniority.	N/A	N/A

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
5.5	High privilege / administrator accounts are appropriately restricted to relevant employees and do not use generic usernames / passwords. (First Line)			⊙	Management has advised that administrator accounts are appropriately restricted, however, there are some administrator accounts where generic user names and complex passwords are shared by more than one senior officer.	5.5.1 All high privilege administrator accounts should be reviewed and refreshed to ensure that all generic user names and passwords are removed, and new unique administrator accounts allocated to all senior officers.	5.5.1 This account will be disabled by June 2018. Owner: Bernie Callaghan Date: 29 June 2018
5.6	Appropriate joiners, movers and leavers procedures have been established to ensure access remains appropriate to role. (First Line)	⊙			Processes are in place for authorisation and approval of new joiners and movers to obtain access to relevant systems. A 'leavers process' is in place to remove and delete access to relevant systems.	N/A	N/A
5.7	There is a regular (at least quarterly) review of all user access rights and privileges to ensure these remain appropriate. (Second Line)			⊙	Management has advised that regular reviews are not performed due to the relatively low levels of staff turnover.	5.7.1 A structured review process should be established an implemented at an appropriate – at least every six months. This review should be performed by the IT team.	5.7.2 A new review framework will be introduced by Sept 2018. Owner: Bernie Callaghan Date: 28 September 2018
5.8	Data loss prevention software is used to highlight and restrict any inappropriate or unusual transfers of data within or outwith the organisation. (First Line)			⊙	Data Loss Prevention (DLP) software is not used by LVJB at present although this is currently being researched by the LVJB IT Manager with a view to future implementation.	5.8.1 Implement appropriate Data Loss Prevention (DLP) software covering the LVJB core network and associated applications.	5.8.1 DLP software will be introduced by the end of 2018. Owner: Bernie Callaghan Date: 21 December 2018

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
5.9	Firewall and related protection arrangements are in place to restrict inappropriate external access to IT systems and applications. (First Line)	⊙			An established firewall product is in place (Sophos Intercept X). This is tested at least annually via independent third-party penetration testing to support ongoing public sector network accreditation.	N/A	N/A
5.10	Structured system monitoring arrangements (such as review of system access logs, unsuccessful log in attempts, unusual network activity, events, or transactions etc) are in place to identify inappropriate access to IT systems and applications. (Second Line)		⊙		Several monitoring processes have been established, however, these have not been consolidated into a structured framework / oversight process	5.10.1 Establish and implement a structured system monitoring framework that specifies the nature and frequency of monitoring to be performed, and the process for escalating; reporting; and resolving any weaknesses identified.	5.10.1 The tool being evaluated at 5.8 also incorporates security and threat detection and will be supported by monitoring and review arrangements undertaken by the Information Security Officer. Owner: Bernie Callaghan Date: 21 December 2018
5.11	Any data with specific government classifications (Official - Sensitive, Secret, Top Secret) is subject to additional security restrictions and measures. (First Line)	⊙			Management has advised that no data is stored by LVJB that falls within these categories.	N/A	N/A
5.12	Email filtering arrangements are in place to reduce the risk of viruses and malware corrupting LVJB systems and networks. (First Line)	⊙			LVJB use Sophos Web Appliance software to monitor and filter incoming email and network traffic for viruses, malware, and other similar threats.	N/A	N/A

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
5.13	Employees can encrypt outgoing and incoming email messages as required.	⊙			Email encryption is not available to LVJB employees. Management has advised that there is limited need to encrypt e mails. Employees do have the ability to password protect individual attachments or ZIP files and send passwords separately. For larger data sharing requirements, LVJB has recently commenced using 'Objective Connect' software which provides a secure data sharing workspace for larger data sets.	N/A	N/A
5.14	Use of USBs and other mobile storage devices is appropriately restricted and controlled. (First Line)	⊙			All USB ports on LVJB desktops and laptops have been disabled and specific permission is required (request via the IT Manager) for any exceptions to this.	N/A	N/A
5.15	Access to LVJB networks, systems and applications from external locations (i.e. working from home / working remotely) is appropriately restricted and controlled. (First Line)		⊙		LVJB employees can access the LVJB corporate network and applications from home or other remote locations using a secure VPN (Virtual Private Network) connection. This facility is restricted to c.10-12 of LVJB's senior personnel and requires specific configuration from the IT Manager via the Windows Active Directory to establish this permission. However, details of the risks and supporting controls associated with home working and virtual private	5.15.1 The ITMS Policy should be updated to reflect the risks associated with storing or retaining electronic or hard-copy documentation at home or at other locations.	5.15.1 The ITMS Policy will be updated by July 2018 Owner: Bernie Callghan Date: 31 July 2018

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
					network (VPN access) access are not recorded in the ITMS policy.		
5.16	LVJB has an established home and mobile working policy that covers control of data on home and personal devices as well as retention of hard copy information at home or other locations. (Second Line)	⊙			Generally, employees are not permitted to access emails or the network from personal mobile devices.	N/A	N/A
5.17	LVJB's home and mobile working policy includes specific focus on the use of personal email accounts. (Second Line)		⊙		The LVJB ITMS policy (Sub Policy 2) prohibits staff from using web-based email accounts or from using personal external email accounts for work-related purposes. However, there are no established processes to ensure that sensitive papers are not sent to Board member Hotmail accounts.	5.17.1 All Board papers being set to Board member Hotmail accounts should be appropriately password protected or encrypted.	5.17.1 Only public documents i.e. Board papers are distributed via the clerk to Board members. As such, management do not consider that there is significant risk in this regard. Risk Accepted
5.18	LVJB systems, networks and applications are subject to regular updates, configuration review and patching (where required). (First Line)	⊙			The WSUS service (Windows Server Update Services) is used to update and configure all Windows software and ensure that required patches and fixes are available for application. LVJB has a 'Vulnerability Management Policy' which outlines the timing and priority of when patches and fixes are applied based on their significance. An additional network scanning and patch management tool (GFI Languard) is also used to support identify and	N/A	N/A

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
					address network patch and vulnerabilities. Other network and VMWare patches are applied manually by the LVJB IT Manager.		
6 Subject access and freedom of information requests							
6.1	Appropriate processes have been established for processing Subject Access (SARs) and Freedom of Information (FOI) requests. (Second Line)	⊙			An established process is in place which is managed by the Secretariat team and subject to overview by the Assessor and Depute Assessor.	N/A	N/A
6.2	SARs and FOI requests are dealt with and managed by an appropriately qualified individual. (First Line)	⊙			Requests are handled by Secretariat and routed to the relevant member of the management team for response.	N/A	N/A
6.3	SARs and FOI requests are responded to within the appropriate time periods. (First Line)	⊙			Management did not indicate any issues with respect to compliance with applicable SAR or FOI response timelines.	N/A	N/A
6.4	SARs and FOI requests are subject to appropriate review and redaction (where required) prior to issue. (First Line)	⊙			All responses to external parties are subject to review by the Assessor and/or the Depute Assessor. Any redactions required would be highlighted at this stage of the process.	N/A	N/A
6.5	KPIs and information on SARs and FOI performance (including failure to reply within required timeframes) are recorded and reported to the	⊙			SAR and FOI information is reported at internal management meetings but not formally covered at Board meetings –	The relevant management action is covered at section 1.6 above.	N/A

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
	Board / Governance Committee (Second Line)				any significant or notable issues would be highlighted where appropriate.		
7 Third Party Data Sharing Arrangements							
7.1	Appropriate arrangements have been established to ensure that data sharing with third parties is compliant and secure. (Second Line)		⊙		<p>Significant volumes of data are shared with relevant local authorities (Edinburgh, East Lothian, Midlothian, and West Lothian); the Scottish Assessors Association; external printers; and a wide range of stakeholders and interested parties.</p> <p>A summary Memorandum of Understanding (MoU) is in place with the main external printer used but formal data sharing agreements are not in place with other key third parties.</p>	<p>7.1.1 Establish formal data sharing agreements with key third parties to ensure that the process applied is compliant with applicable regulations and secure.</p> <p>These should include (but not be restricted to):</p> <ul style="list-style-type: none"> Clearly defined roles and responsibilities for the data sharing process; A clearly defined escalation and resolution process to be applied in the event of any issues or breaches. The Board should be made aware of all significant data sharing arrangements with third parties. 	<p>7.1.1 Management have commenced the creation of Data Sharing Agreements and key contract reviews are currently underway to align with impending GDPR requirements.</p> <p>Owner: Bernie Callaghan Date: 1 December 2018</p>
8 Data Breaches							
8.1	Response plans are in place for dealing with data breaches or data losses.		⊙		The ITMS Policy does not include a specific section covering actions	8.1.1 Update / modify the ITMS Policy to include the process to be applied in	8.1.1 The ITMS policy will be updated by July 2018. Owner: Bernie Callaghan

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
	(Second Line)				required in the event of a significant data breach or loss incident.	<p>the event of a significant data breach or data loss incident. This should include, but not be restricted to:</p> <ul style="list-style-type: none"> • Roles and responsibilities of employees and senior officers; • Responsibility for reporting significant breaches to the Information Commissioner's Office; • The process for communicating the breach to any impacted third parties; and • Frequency of testing incident plans. 	Date: 27 July 2018
8.2	Relevant training to support incident response plans has been developed and delivered. (Second Line)			⦿	See comments at 8.1 above	See recommendation at 8.1 above.	See 8.1
9 GDPR Readiness							
9.1	A GDPR preparation and implementation plan has been established. (Second Line)	⦿			The Governance Manager has developed an outline GDPR preparation and implementation plan.	N/A	N/A
9.2	Privacy notices have been reviewed and updated in line with GDPR requirements. (Second Line)	⦿			The Governance Manager has drafted updated privacy notices and is in the process of finalising these.	N/A	N/A

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
9.3	A comprehensive GDPR gap analysis has been undertaken. (Second Line)	⊙			<p>An assessment of GDPR requirements in comparison to current operational processes has been performed.</p> <p>Whilst this has not been fully documented, the assessment has not highlighted any significant gaps that are not already being addressed by management.</p> <p>The Governance Manager is attended a 4-day GDPR course at the end of March 2018 and will use this as an opportunity to consider whether any additional action is required.</p>	<p>9.3.1 Known GDPR compliance gaps should be documented together with supporting action plans, and presented to the Board.</p> <p>This paper should also include details of any additional resources to address the gaps identified.</p>	<p>9.3.1 This will be presented at the September 2018 Board meeting.</p> <p>Owner: Graeme Strachan Date: 3 September 2018</p>
10 Business Change Projects							
10.1	Data privacy considerations are fully reflected in business change projects. (First Line)	⊙			<p>Management has advised that there have been no recent business or system change projects which presented significant impacts from a privacy or data protection perspective.</p> <p>Whilst the Transformation and Cultural Change Project (TCCP) was significant, it did not involve any substantive change or new use of personal data.</p> <p>Business changes associated with the Barclay Review and the proposed Tram Extension are more likely to involve data privacy considerations.</p>	10.1.1 Data privacy considerations should be included in planning for the Barclay and Tram Extension projects.	Complete: Data Privacy Impact Assessments are already embedded in the Project Initiation Documents for Barclay and Tram Extension projects
10.2	Privacy by Design (PBD) and Privacy Impact Assessment (PIA) methodologies are used to support key business change projects.	⊙			The Governance Manager is familiar with the Privacy by Design (PBD) and Privacy Impact Assessment (PIA) methodologies and will ensure that	10.2.1 PBD and PIA methodologies should be documented and shared with other employees to	See 10.1.1 above.

Ref	Expected Control	Established			Observation	Recommendation	Agreed Management Action and Timeframes
		Y	P	N			
	(Second Line)				these are applied to future business change projects.	mitigate any potential key person dependency risk.	

Appendix 2 - Basis of our Classifications

Finding rating	Assessment rationale
Critical	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Critical impact on operational performance; or • Critical monetary or financial statement impact; or • Critical breach in laws and regulations that could result in material fines or consequences; or • Critical impact on the reputation or brand of the organisation which could threaten its future viability.
High	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Significant impact on operational performance; or • Significant monetary or financial statement impact; or • Significant breach in laws and regulations resulting in significant fines and consequences; or • Significant impact on the reputation or brand of the organisation.
Medium	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Moderate impact on operational performance; or • Moderate monetary or financial statement impact; or • Moderate breach in laws and regulations resulting in fines and consequences; or • Moderate impact on the reputation or brand of the organisation.
Low	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Minor impact on the organisation's operational performance; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or • Minor impact on the reputation of the organisation.
Advisory	<p>A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.</p>

Appendix 3 – Terms of Reference

Lothian Valuation Joint Board

Terms of Reference – Review of Data and Records Management Arrangements

To: Graeme Strachan, Principal Assessor; Bernie Callaghan, Governance Manager

From: Lesley Newdall, Chief Internal Auditor; Paul McGinty, Principal Audit Manager

Date: 12/02/18

This Internal Audit review is undertaken as part of the Lothian Valuation Joint Board Internal Audit coverage plan for 2017/18. Given the financial, fiscal and democratic importance of the registers managed and maintained by LVJB, there is obviously a clear expectation that LVJB's arrangements for data and records management are robust and fully in line with good practice. As such, as part of the Internal Audit coverage for 2017/18, senior officers requested that we ensure some focus on overall data and records management arrangements.

Scope

Based on the planning discussions outlined above, we agreed that we would undertake a high level 'baseline' assessment of LVJB's broad data and records management arrangements. This involved consideration of the following aspects:

- Overall Policy and Governance
- Training and Awareness
- Data Assets and Flows
- Data Retention and Destruction
- Data Access and Security
- Subject Access Requests
- Freedom of Information Requests
- Third Party Data Sharing
- Data Breaches
- GDPR Preparation and Compliance
- Business Change Projects
- IT Security Risk Considerations.

Approach

Our approach involved:

- Meetings, interviews and inquiries with relevant managers and officers to understand current arrangements
- Review of relevant policies, procedures, documentation and management reports
- Use of our baseline control assessment framework model to compare expected controls, activities and procedures with current arrangements (see Appendix 1)
- Highlighting any identified gaps or opportunities for improvement for management consideration and action.

Scope Limitations

It should be noted that our assessment at this stage represents a high-level baseline review of current arrangements – we have not undertaken testing of the effectiveness of existing controls as part of this review. The framework outlined in Appendix 1 can be further developed and refined in subsequent periods and used to provide the basis for targeted first, second and third-line testing* as required.

In 2014/15 LVJB obtained accreditation to access certain services (such as the Cabinet Office Individual Electoral Registration Digital Service) over the Public Services Network (PSN). PSN is the UK Government's secure high-performance network and access to use it requires LVJB to demonstrate compliance with a range of IT security requirements proscribed by the Cabinet Office. This also requires LVJB to commission an annual Network Penetration Test and IT Security Healthcheck from a Crest accredited advisor and to submit an annual compliance confirmation to the Cabinet Office. Our work has not sought to repeat or re-assess any aspect of PSN compliance (or the external Penetration Test or Healthcheck) as part of this exercise

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	Lesley.Newdall@edinburgh.gov.uk
Paul McGinty	Principal Audit Manager	Paul.McGinty@edinburgh.gov.uk

Key Contacts

Name	Title	Role	Contact Details
Bernie Callaghan	Head of Governance	Key Contact	Bernie.Callaghan@lothian-vjb.gov.uk
Graeme Strachan	Principal Assessor	Review Sponsor	graeme.strachan@lothian-vjb.gov.uk

Lothian Valuation Joint Board

Internal Audit Report

Review of LVJB Business Rates Internal Assurance Framework

27 August 2018

LVJB1702

Contents

1. Background and Scope	2
2. Executive Summary	3
3. Detailed Findings and Agreed Management Actions	4
Appendix 1 – Valuation Roll – Risk and Control Assessment	8

This Internal Audit review is undertaken as part of the established service level agreement with the Lothian Valuation Joint Board that covers provision of Internal Audit services by the City of Edinburgh Council.

The review is designed to help the Lothian Valuation Joint Board assess and refine its internal control environment. It is not designed or intended to be suitable for any other purpose and should not be relied upon for any other purpose or by any other party.

The internal audit work and reporting has been performed in line with the requirements of the Public Sector Internal Audit Standards (PSIAS) and as a result is not designed or intended to comply with any other auditing standards.

Whilst a number of specific recommendations included in this report to strengthen internal control, it is management's responsibility to design, implement and maintain an effective control framework, and for the prevention and detection of irregularities and fraud.

This is an essential part of the efficient management of the City of Edinburgh Council. Communication of the issues and weaknesses arising from this audit does not absolve management of this responsibility. High and Critical risk findings will be raised with senior management and elected members as appropriate

1. Background and Scope

Background

The Lothian Valuation Joint Board (LVJB) is a statutory entity established under the 1995 Valuation Joint Boards Order. LVJB provides a range of specialist valuation and electoral registration services for the Edinburgh; East Lothian; West Lothian; and Mid Lothian local authorities, and is responsible for the management and ongoing and administration of their Business Rates Valuation Rolls; Council Tax Valuation Lists; and Electoral Registers.

LVJB delivers these services on an operating budget of c.£6m, but generate circa £600m of Business Rate and Council Tax revenue across for local authorities.

The financial, fiscal, and democratic significance of the activities performed by LVJB reinforce the need to ensure that they have strong operational controls that are adequately designed; operate effectively; and are and consistently applied, with supporting governance and assurance frameworks.

Operational control; governance; and assurance frameworks can be considered in the context of the three lines of defence model where the first line is those employees responsible for applying controls when performing operational processes; the second line is those responsible for defining the frameworks and policies that apply to operational processes and assessing ongoing compliance with them; with the independent third line responsible for providing assurance that the framework is appropriately designed and operating effectively.

All amendments to LVJB's core registers are subject to review and checking by (first line) team members. Additionally, there is a small team of two (second line) employees who provide internal assurance across the three core areas of LVJB's operations outlined above.

LVJB receives (third line) Internal Audit services from both the City of Edinburgh Council who provide assurance on key operational controls; and their external auditors (Scott Moncrieff) who provide assurance on financial controls; with the outcomes of their work provided to the LVJB Board. Additional assurance is also provided by external third parties, for example, the independent third party assurance provided on IT security to confirm ongoing compliance with the Scottish Government's Public Sector Network requirements).

Scope

Our review was performed as at **31 March 2018**, and focused on the adequacy of design of the business rates valuation governance and assurance framework. The objective of the review was to:

- Assess the adequacy of the design of existing internal assurance arrangements; and
- Identify opportunities to further improve and develop these arrangements;

Scope Limitations

The Council Tax and Electoral Register governance and assurance frameworks were specifically excluded from the scope of our review.

2. Executive Summary

Our review confirmed that the business rates internal assurance framework is generally adequate, with enhancements required. This assessment is based on the outcomes of our review; the fact that there have been no significant issues identified with the completeness and accuracy of source business rates valuation data; and no significant valuations errors.

Whilst LVJB has an established first and second line business rates valuation assurance framework, it is not currently used efficiently and effectively as resources are not focused on the most significant risks associated with maintaining the valuation roll and calculating rateable values.

Consequently 10 findings have been raised (8 medium and 2 low) highlighting the need to improve the internal assurance framework. Addressing these findings will ensure that first and second line assurance over the operational and system controls supporting maintenance of the valuation roll and valuations calculations is strengthened to mitigate more effectively exposure to the risks associated with these processes.

Further detail on the findings raised are included at Section 3 below - [Detailed Findings and Agreed Management Actions](#); and with further supporting detail on the risk and control assessments performed at [Appendix 1 – Valuation Roll – Risk and Control Assessment](#).

Once implemented, LVJB would also derive benefit from implementing similar risk based assurance frameworks across the Council Tax and Electoral Register teams.

Finally, it is recommended that progress with implementation of these findings is monitored via the new Governance Committee, with regular progress updates provided to the Board.

Internal audit will also review the full population of the High and a sample of the moderate rated actions as part of the 2019/20 LVJB review to confirm that they have been effectively implemented and sustained.

3. Detailed Findings and Agreed Management Actions

Rating	Initial Observation / Recommendation	Agreed Management Action and Date	X Ref to App 3
Medium	<p>1. Business Rates Assurance Framework</p> <p>LVJB should develop and implement an appropriate risk based business rates valuation assurance framework that is applied across the operational processing (first line) teams and assurance (second line) teams.</p> <p>This model should include first line assurance checks performed by operational management, and review of those management checks performed by second line assurance teams.</p> <p>Sampling methodology should be developed and implemented to support the framework, detailing the number (based on volumes) and nature of roll changes and rateable value calculations to be reviewed, with focus on the most significant risks associated with maintaining the valuation role and calculating rateable values.</p> <p>This could include (for example) additional review of higher risk properties; higher risk property classes; and highly valued properties with fewer checks performed on lower risk properties and roll changes.</p> <p>Meaningful thresholds and limits such as <£15,000; £15,001 - £18,000; and £18,001 - £35,000 should also be considered as small business relief levels can be applied to properties where rateable values fall within these categories. Some further areas for consideration are included at Appendix 3.</p> <p>The volume and depth of checks to be performed should consider resource availability; the skills and experience of the first line (operational) team members with (for example) more focus on new starts or poor performers; and ensure appropriate rotation and segregation of duties in checking responsibilities.</p> <p>Management should also consider the whether it would be beneficial to implement external quality assurance checks in collaboration with other valuation boards on a reciprocal basis.</p> <p>Once implemented, management should also consider extending this framework to Council Tax and Electoral Register processes.</p>	<p>LVJB is progressing with an improved Governance and Assurance model and will take account of the elements outlined in Appendix 3.</p> <p>This shall be raised through the Scottish Assessors Association with a view to establishing the possibility of reciprocal review processes.</p> <p>Head of Governance – Dec 2018</p>	E; F; G; S; Y
Medium	<p>2. Governance Framework</p> <p>The new Governance Committee should be constituted in line with Audit Committee good practice - a number of 'good practice' and guidance documents have been shared with LVJB to assist with the development of the Governance Committee remit / terms of reference.</p>	<p>The new Governance Committee will be constituted by May 2018 with a formal remit which takes account of these good practice and guidance documents.</p>	AA

	<p>Detailed Internal Audit and other assurance reports should be circulated to the new Governance Committee with summaries provided to the Board where appropriate.</p>	<p>Detailed Internal Audit reports will be circulated to the new Governance Committee with summaries provided to the Board.</p> <p>Head of Governance – May 2018</p>	
Medium	<p>3. Business Rates Avoidance Processes</p> <p>LVJB should document the current processes applied to mitigate against the key risk of business rates avoidance, considering the processes and controls applied by local authorities (for example, notification of new buildings developed with no planning consent).</p> <p>Emphasis should be placed on the processes to be applied to establish the correct effective date from which Rateable Value increases apply.</p> <p>This will provide the opportunity to assess whether these processes are adequate or whether additional measures should be considered.</p> <p>There may be merit in considering recent developments in England where LVJB management highlighted that many businesses have evolved their 'business rates avoidance' controls.</p>	<p>Agreed. The framework of current arrangements will be documented assessed and reported. Specific consideration will be given to the areas noted opposite.</p> <p>Head of Governance – Dec 2018</p>	A
Medium	<p>4. Local Authority Source Data Filtering</p> <p>Management should ensure that the new process for manually filtering planning permission, building warrant and completion certificate information received from local authorities is fully assessed prior to implementation, as there is a risk that information that could impact the rateable value could be inadvertently filtered.</p> <p>The process should be documented, and clear guidance provided on the nature of information that will not impact rateable values and can be ignored.</p> <p>It will also be important to ensure appropriate segregation of duties in the filtering process.</p> <p>Sample based checking should also be applied to the filtering process to ensure that no significant error have been made.</p>	<p>Agreed. These aspects will be considered as part of the implementation of the new arrangements.</p> <p>Head of Governance – May 2018</p>	B; M
Medium	<p>5. Performance and Exception Reporting</p> <p>Management should consider how existing business rates valuations operational performance reporting could be improved to provide a clearer view of performance.</p> <p>Management should also consider reporting on potential 'Tax Loss' situations where an increase in Rateable Value has been 'delayed' into a subsequent fiscal year thus limiting the ability to apply an increase in Rateable Value for the entire period since the change occurred.</p>	<p>Agreed. Management have already commenced work in this respect and intend to establish a suite of such reporting – in developing this we will assess our longer-term requirements for data analytics and wider reporting.</p>	C; G; J; K; L; N; R; T; Z

	<p>Additionally, regular exception reporting should be developed and implemented detailing any unusual or exceptional transactions processed, for example: unusual reductions in rateable value; changes close to applicable small business relief thresholds; 'delayed' projects; and instances where expected changes in Rateable Value do not occur.</p> <p>These exception reports could also include 'alerts' to highlight transactions which are approaching key deadlines.</p> <p>Finally, management should consider use of data analytics to support sample selection for the assurance process; and identification of any unexpected anomalies in the valuation roll.</p>	Head of Governance – Dec 2018	
Medium	<p>6. Spreadsheet Model Guidance and Oversight</p> <p>LVJB should establish general guidance on creating, maintaining, and reviewing spreadsheet models. Guidance should include, but should not be restricted to:</p> <ul style="list-style-type: none"> • use of password protection to ensure the spreadsheet cannot be accessed and amended in error; • use of cell protection to protect complex macros and formulae; • the requirement to document assumptions and rationale supporting the model; • Details of any external evidence provided to support the calculations; and • Protocols for naming and filing these spreadsheets so that they can be easily located in the event of a rateable value calculation. <p>The process for risk based independent review and validation of spreadsheets should also be documented. It is important that this validation process is applied prior to generation of final rateable value calculations.</p>	<p>Agreed. New arrangements will be implemented in this regard.</p> <p>Head of Governance – Dec 2018</p>	D
Medium	<p>7. Corporate Policies – Employee Inducement and Conflicts of Interest</p> <p>Management should consider whether adequate corporate policies; procedures; and employee guidance; have been established in relation to situations where employees could be subject to inappropriate influence or inducement when assessing the Rateable Value of individual properties.</p>	<p>A review will be undertaken to assess the adequacy of our current policies and arrangements in this regard.</p> <p>Head of Governance – Dec 2018</p>	L
Medium	<p>8. User Entitlement Reviews</p> <p>A quarterly / six-monthly review of all access permissions and authorities on the CVS / Civica systems should be implemented to ensure that these remain appropriate and that access is appropriately restricted to relevant modules / sections of the system in line with employee roles and levels of seniority.</p>	<p>Agreed. This will be established.</p> <p>Head of Governance – Sep 2018</p>	O; P; Q
Low	<p>9. Third Party Documentation supporting Valuations</p>	<p>Professional valuation staff apply experience and judgement to a range of information</p>	H

	<p>Management should consider whether there would be benefit in establishing clear guidance as to what is acceptable from, and what reliance can be placed upon, documentation provided by third parties.</p> <p>For example, are all certifications by Advisors worthy of equal reliance, and are distinctions drawn between certification reports provided by 'Accountants' and 'Chartered Accountants'?</p>	<p>sources to support valuation decisions. The creation of baseline standards shall be considered as part of ongoing changes and improvements.</p> <p>Head of Governance – June 2018</p>	
Low	<p>10. Best Practice Sharing with Local Authorities</p> <p>The LVJB Governance team should consider meeting with the local authority Assessment Roll teams to gain a more informed and detailed understanding of how weekly interface files are used for reconciliation purposes at local authority level and to identify opportunities for incremental improvement and development in current arrangements.</p>	<p>Agreed. We will seek to have a first round of meetings by Sep 2018.</p> <p>Head of Governance – Dec 2018</p>	

Appendix 1 – Valuation Roll – Risk and Control Assessment

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
A	Risk that properties are not included on the Valuation Roll.	<p>The historical basis of the Valuation Roll and processes established to capture new properties (refer below) make it unlikely that existing properties would consistently excluded from previous quinquennial revaluation exercises.</p> <p>Some property categories (for example ATMs, mobile masts; construction portacabins; or stalls in shopping malls) could be established with no formal notification (Senior officers explained that such risk trends are generally picked up on by LVJB professionals.</p> <p>Management has also confirmed that a number of compensating controls exist, such as the vigilance and local knowledge of LVJB professionals; or adjacent owners advising re any new properties.</p> <p>Some properties are also excluded from the Valuation Roll - such as agricultural properties.</p>	Finding 3	<p><u>Second Line</u></p> <p>Regular review to confirm that processes are consistently applied by all valuers.</p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
B	<p>New properties are built, but are not added to the Valuation Roll.</p> <p>OR</p> <p>New properties are built but are not added to the correct local authority Valuation Roll.</p>	<ol style="list-style-type: none"> 1. New properties are legally required follow local authority planning, building warrant and completion certificate approval processes. Consequently, LVJB receives weekly updates on planning permission; building warrants; and completion certificates from each local authority that are used to update to update the roll. 2. Where new properties are built without securing the necessary planning or building warrant permissions, compensating controls include local knowledge of LVJB professionals or adjacent owners making LVJB or the local authority aware of any new properties. 3. A weekly reconciliation is performed between details of planning and building warrant applications and completion certificates and the relevant local authority valuation rolls to confirm that they are complete and accurate, with any exceptions identified addressed and resolved. 	Finding 4	<p><u>Second Line</u></p> <p>Regular sample testing by second line assurance teams to confirm that the filtering process is consistently applied in line with guidance.</p> <p>Any exceptions should be recorded and discussed with the teams performing the filtering exercise.</p>
C	<p>A property is changed (as described at 2 above) but this is not reflected on the Valuation Roll on a timely basis.</p> <p>OR</p> <p>An inaccurate 'effective date' is applied.</p>	<ol style="list-style-type: none"> 1. LVJB's main responsibility is to ensure that it accurately reflects the change in the Valuation Roll and the Effective Date of the change and communicates this to the local authority. Management reporting on elapsed time between the Effective Date of the assessment and the change recorded on the Valuation Roll is provided each month to the LVJB Corporate Leadership Team. 2. Valuers are required to include explanations on the CVS system for any changes processed more than 3 months after the effective assessment date. This report is also provided to the monthly Corporate Leadership team meetings. 	Finding 5	<p><u>First Line</u></p> <p>Review of performance reporting by first line assurance teams and investigation of any items that seem unusual or do not meet any expectations.</p> <p>The outcomes of these reviews and investigations should be documented.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks to ensure that they are performed effectively, with focus on ensuring that explanations for any anomalies are adequate</p> <p>Testing to confirm the ongoing accuracy of KPIs included in the performance reports.</p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
D	Rateable Value calculations are incorrect.	<ol style="list-style-type: none"> The majority of RV calculations are performed calculations by CVS system. If there were underlying errors in the CVS system it is likely that these would have been identified already, as a significant volume of RV's would be incorrectly calculated. For more complex properties, RV calculations are performed in separate spreadsheets with the numbers calculated then entered into CVS. A senior colleague is unlikely to cross-check and recalculate every element of an underlying spreadsheet (which is understandable) but will apply professional judgement and experience to the review process as appropriate. 	Finding 6	<p><u>First Line</u></p> <p>Review of accuracy of spreadsheet calculations prior to entry into the CVS system.</p> <p><u>Second Line</u></p> <p>Review of a sample of spreadsheet models to ensure that they are developed and maintained in line with guidance.</p> <p>Review of ongoing accuracy of CVS RV calculations.</p>
E	Rateable Value calculation includes errors as a result of an incorrect application of the relevant Valuation Rules / Practice Notes.	<ol style="list-style-type: none"> The valuation process is supported by a detailed framework of guidance and practice notes as well as the ability to consult with colleagues internally or at other Valuation Boards. Errors in the application of technical guidance would be made in the first instance by the employee performing the valuation, and then remain undetected by the more senior employee performing an independent review. Reliance on the professional judgement, diligence and experience of the employee performing the valuation calculation and the senior person reviewing the calculation. <p>LVJB management is at the early stage of planning a move away from a full secondary review model to a more risk-based approach. Secondary review of all transactions / changes has been a core part of LVJB's approach (and culture) for many years – and it will be important to assess the risks and practicalities associated with moving to a new arrangement where this is not the case.</p>	Finding 1	<p><u>First Line</u></p> <p>Regular risk based reviews by Senior employees prior to completion of changes and calculation of RV to ensure that processes and guidance have been applied.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks to confirm that they are being performed effectively and all exceptions identified and resolved.</p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
F	Properties are incorrectly valued due to complexity, size, or the specialised nature of the property (such as plant or machinery valuations or other specialist factors). Main risk is undervaluation as rate payer has right of appeal if valuation is perceived as being too high.	Professional judgement, experience and diligence of the employee performing the valuation calculation and the more senior person reviewing the calculation.	Finding 1	<u>First Line</u> Regular risk based reviews by Senior employees prior to completion of changes and calculation of RV to ensure that processes and guidance have been applied. Regular review of performance reporting to identify any instances of undervaluation for subsequent investigation. <u>Second Line</u> Review of a sample of first line checks to confirm that they are being performed effectively and all exceptions identified and resolved.
G	Rateable Value calculations are incorrect due to incorrect measurements / dimensions / size of the property as recorded on CVS.	<ol style="list-style-type: none"> 1. Management has advised that 'clerical errors' can occur despite reliance on the professionalism and diligence of the team members; existence of guidance and practice notes; and first line reviews. 2. If a clerical error resulted in a material or recurring error in Rateable Value, LVJB does have the option of revisiting this and revising the Effective Date (albeit such instances would be very rare). 	Finding 1 Finding 5	<u>First Line</u> Regular risk based reviews by Senior employees prior to completion of changes and calculation of RV to ensure that processes and guidance have been applied. <u>Second Line</u> Review of a sample of first line checks to confirm that they are being performed effectively and all exceptions identified and resolved.
H	Underlying information provided by third parties used for Rateable Value calculations is incorrect.	<ol style="list-style-type: none"> 1. LVJB has legal authority to request a range of relevant rental and financial information from these parties. 2. Information provided is often supported by certifications and correspondence from other parties such as Financial Advisors or Accountants 	Finding 9	<u>First Line</u> Review of documentation provided by third parties to confirm authenticity and accuracy prior to completion of RV calculation. <u>Second Line</u>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
	OR Properties that do not exist are included on the Valuation Roll.	3. Professional judgement of the valuers to assess and consider this information with respect to accuracy / reliability. 4. Comparison to other similar properties 5. Second review by senior team member		Review of a sample of first line checks to confirm that they are being performed effectively and all exceptions identified and resolved.
I	Other information (for example Owner, Tenant, Proprietor) recorded on the Valuation Roll is incorrect.	LVJB is responsible for the Valuation Roll and local authorities are responsible for the Assessment Roll. Local authorities rely upon LVJB for Rateable Value and Effective Date data and are less concerned with other fields such as they use data in their own systems to generate bills. Local authorities currently do not share their more up to date information with LVJB. In practice, this means that LVJB will, on some occasions, be issuing incorrect correspondence (such as Valuation Notices). The scale of this issue is not easy to quantify but LVJB management are engaged in discussions with local authority partners to address this.	Finding 10	N/A
J	Information regarding reliefs, allowances or discounts which impact rates recovery are inaccurate or incorrect.	1. Responsibility for managing all reliefs and discounts regarding commercial rates is the responsibility of the relevant local authority. LVJB's core responsibility remains the Rateable Value and the effective date. 2. It was noted that the Small Business Bonus Scheme that provides business rates relief applies to properties with Rateable Values of <£15,000; £15,000-£18,000; and £18,000-£35,000. In terms of LVJB's consideration of exception and analytical reporting, there may be some merit in considering valuation trends and practices in relation to these values.	Finding 5	<u>First Line</u> Review of exception reports to identify any odd or unusual reductions in RVs that reduce thresholds sufficiently to qualify for discounts or relief, and perform checks to supporting documentation. <u>Second Line</u> Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
K	Inappropriate or unauthorised amendments made to the Valuation Roll.	<ol style="list-style-type: none"> Changes would be made by a member of the LVJB team and then subsequently reviewed and approved by a second more senior team member. Consequently, collusion would be required. Reductions in Rateable Value would tend to 'be of interest' and therefore subject to close scrutiny when checked as part of the secondary review process. <p>We did note that there is no 'separate' or selective checking of reductions in Rateable Value or, for example, a weekly or monthly exception report of detailing all reductions in Rateable Value.</p>	Finding 5	<p><u>First Line</u></p> <p>Review of exception reports to identify any odd or unusual reductions in RVs that reduce thresholds sufficiently to qualify for discounts or relief and check these to supporting documentation.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.</p>
L	LVJB employees are subject to inappropriate influence in performing their duties.	<ol style="list-style-type: none"> Professionalism of the LVJB personnel. Collusion would be required as any inappropriate undervaluation changes would need to be processed by a member of the LVJB team, and then subsequently reviewed and approved by a second more senior team member. 	Finding 5 Finding 7	<p><u>First Line</u></p> <p>Review of exception reports to identify any odd or unusual reductions in RVs that reduce thresholds sufficiently to qualify for discounts or relief and check these to supporting documentation.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.</p> <p>Obtain confirmation that all employees have read and understood policy and guidance on an annual basis.</p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
M	LVJB employees are subject to inappropriate influence to remove or exclude properties or amend their details.	<ol style="list-style-type: none"> 1. Professionalism of the LVJB personnel. Collusion with senior reviewer would also be required. 2. LVJB has implemented a new manual process where planning permission, building warrant and completion certificate information is 'filtered' in advance by a Divisional Valuer and therefore may not be uploaded into Civica / CVS if considered immaterial <p>This is an important process change and could increase the risk that changes in Rateable Value are not reflected on the Valuation Roll (as there would be no separate indication that a change in value had occurred if it was manually filtered out).</p>	Finding 4	<p><u>Second Line</u></p> <p>Review of the data filter process to ensure that it is being applied in line with applicable guidance.</p>
N	Inappropriate amendments are made to the Valuation Roll in error	<ol style="list-style-type: none"> 1. Reliance on the professional experience and diligence of those with access to the CVS system i.e. that errors or mistaken entries are not made. 2. All changes are currently subject to secondary review and checking by a more senior colleague - therefore any obviously incorrect or mistaken entries should be identified through this review. 3. A daily report of all transactions processed within each team is also available from the CVS system for each Team Manager - as such, review of this report would provide another opportunity to identify any obviously incorrect entries which had not been identified via secondary review and checking. 	Finding 5	<p><u>First Line</u></p> <p>Review of exception reports to identify any odd or unusual reductions in RVs that reduce thresholds sufficiently to qualify for discounts or relief and check these to supporting documentation.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.</p>
O	Inappropriate access to the Valuation Roll.	<ol style="list-style-type: none"> 1. Access to the Civica and CVS applications is controlled through the Windows Active Directory network management system. 2. Network access is controlled through username and password. An additional user name and password access is required to enter the Civica application whilst network access provides a single sign on to the CVS system. 	Finding 8	<p><u>First Line</u></p> <p>Review of team system access rights to confirm that all leavers have been removed; new starts have been allocated appropriate access rights; and that systems access has been updated to reflect internal changes.</p> <p><u>Second Line</u></p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
		3. There is currently no structured or regular review of user access rights across the Civica and CVS applications on an ongoing basis.		Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.
P	Employees obtain access to elements or modules of the CVS system which they should not have access to.	<ol style="list-style-type: none"> 1. Network rights and permissions are controlled by the IT Department with approvals for new joiners and changes required from relevant Departmental / Line Managers. 2. Access permissions within Civica and CVS are based on job roles with specific settings available for different levels and modules of access. (Civica has more granularity in this respect than CVS). 	Finding 8	<p><u>First Line</u></p> <p>Review of team system access rights to confirm that all leavers have been removed; new starts have been allocated appropriate access rights; and that systems access has been updated to reflect internal changes.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.</p>
Q	Unauthorised or inappropriate access is obtained due to weak or ineffective password or access controls.	<ol style="list-style-type: none"> 1. Windows Active Directory password settings are in place as a first line of defence in this regard. 2. An additional username and password access is required for the Civica system. 	Finding 8	<p><u>First Line</u></p> <p>Review of team system access rights to confirm that all leavers have been removed; new starts have been allocated appropriate access rights; and that systems access has been updated to reflect internal changes.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.</p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
R	Changes to the Valuation Roll are complete and accurate but are not made on a timely basis.	<ol style="list-style-type: none"> 1. Daily reports are generated from the CVS system that show the activity and changes made the previous day. 2. Team Managers receive an auto-email report with visibility of the changes being processed by their team members. 3. The Civica system provides a series of queues and intrays which show the work flow and status across the various teams. 4. Management has overall visibility of volumes and status as well as the ability to search flexibly on a wide range of criteria. 5. No 'alert' reports have been established detailing actions due within specific timeframes, or transactions awaiting review. 	Finding 5	<p><u>First Line</u></p> <p>Review of exception reports to identify any odd or unusual reductions in RVs that reduce thresholds sufficiently to qualify for discounts or relief and check these to supporting documentation.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.</p>
S	Secondary / senior review of changes to the Valuation Roll fails to identify errors or inaccuracies.	<ol style="list-style-type: none"> 1. All changes to the system require a second review by a more senior team member (within the same team) which is recorded and noted in the CVS system ensuring there is a clear audit trail for the review of all transactions. 2. Risk that the review process could become a 'rubber stamping' or token gesture process - ultimately this is down to the professionalism of the individuals involved in the review process. 3. Management is considering implementation of new arrangements where certain lower risk transactions may not be subject to secondary review albeit this is not fully developed or implemented yet. 	Finding 1	<p><u>First Line</u></p> <p>Regular risk based reviews by Senior employees prior to completion of changes and calculation of RV to ensure that processes and guidance have been applied.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks to confirm that they are being performed effectively and all exceptions identified and resolved.</p>
T	Management information and KPIs generated are not accurate or robust.	Current management reports focus upon timeliness and volume of changes made to the Valuation Roll - with a strong focus on changes processed more than 3 months or more than 6 months after the effective date. Reports focus on volume and timeliness by person and by team.	Finding 5	<p><u>First Line</u></p> <p>Review of exception reports to identify any odd or unusual reductions in RVs that reduce thresholds sufficiently to qualify for discounts or relief, and perform checks to supporting documentation.</p> <p><u>Second Line</u></p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
				Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.
U	Third party reports and KPIs produced by LVJB are incomplete or inaccurate.	<ol style="list-style-type: none"> 1. Management has advised that there are few bespoke reports or outputs generated for specific third parties. 2. Some specific data sets are provided to the Scottish Government. 3. A number of third parties (for example Equifax or Scottish Water) make significant use of and rely upon the underlying Valuation Roll data sets - this underlines the importance of the Valuation Roll as the de facto data set for commercial property. 	No finding raised	N/A
V	Data transmission / data interface to local authorities is incomplete, inaccurate, or subject to error.	<ol style="list-style-type: none"> 1. The Valuation Roll interface files comprise 6 main data fields: 1 Inserts (new properties added); 2 Amends (changes to Rateable Values); 3 Deletion/Amends; 4 Name Changes (changes to name of owner / tenant); 5 Property Number Changes; 6 Deletes (properties removed or demolished). 2. CEC has advised that the principal data field transferred into the CEC Northgate iWorld system is the Rateable Value - in general, other data fields (such as owner or tenant) are not used. 3. On some occasions, data may be rejected (e.g. if a data field is already populated). A 'receipt' email file is received from the constituent councils and is saved in the LVJB Interface file email tray. LVJB staff explained that very occasionally a notice may be withdrawn from the interface report if an error or oversight is identified by one of the valuers after the interface file has been sent. On such occasions, IT would be contacted to rectify the matter. 4. A weekly check is in place where LVJB staff confirm that the interface files have been sent to each local authority by auto-email. 	No findings raised	N/A.

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
		<p>An email read receipt is received and this is saved as confirmation that the file has been received by the relevant local authority.</p> <p>Local authorities are not contacted unless there is a specific issue or problem with the interface file - this is very rare.</p>		
W	Data is not adequately protected or secured and could be lost, corrupted, or inappropriately accessed / deleted.	<p>Management has advised that there is robust on-site and off-site back up and IT continuity arrangements have been established.</p> <p>A framework of IT access and security controls is in place.</p>	No findings raised	N/A
X	Data recorded on the CVS system is subject to a cyber or ransomware attack or similar security incident or similar issue.	A framework of IT access and security controls is in place which includes firewalls and email filtering.	No findings raised	N/A

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
Y	Management and maintenance of the Valuation Roll is not subject to appropriate internal or external assurance	<ol style="list-style-type: none"> 1. The current internal assurance activities performed are narrowly focused on the weekly interface file process and a few other targeted areas. 2. Current assurance activities are not risk-based; take place after transmission of interface files; are not supported by a clearly defined assurance framework; and provide limited assurance to senior management. 3. We understand that a full 'changes' report showing all the detailed changes is also generated from the system but this is not used by the internal assurance team. 4. LVJB third line independent assurance is provided by Scott Moncrieff as External Auditors focusing on focuses financial controls and CEC Internal Auditor who provide one review per annum. 5. There is no other independent third party quality assurance provided in relation to operational processes. 	Finding 1	<p><u>First Line</u></p> <p>Regular risk based reviews by Senior employees prior to completion of changes and calculation of RV to ensure that processes and guidance have been applied.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks to confirm that they are being performed effectively and all exceptions identified and resolved.</p>
Z	Data analytics or other information analysis tools are not used to inform, assess, and scrutinise the governance, control, and performance of the Valuation Roll process.	<ol style="list-style-type: none"> 1. Management has confirmed that there is opportunity to interrogate, analyse and report upon the data sets in Civica and CVS. 2. There is currently limited focus on use of data analytics, data mining, or exception reporting to analyse data or generate exception reports. 	Finding 5	<p><u>First Line</u></p> <p>Review of exception reports to identify any odd or unusual reductions in RVs that reduce thresholds sufficiently to qualify for discounts or relief and check these to supporting documentation.</p> <p><u>Second Line</u></p> <p>Review of a sample of first line checks on performance reports to confirm that they are being performed effectively with any potential anomalies investigated.</p>

#	Process Risk	What controls currently mitigate this risk?	X Ref to Section 3 - Detailed Findings	Suggested Internal Assurance Checking
AA	Management and maintenance of the Valuation Roll is not subject to appropriate governance and scrutiny arrangements through the LVJB Board or other Committees.	<ol style="list-style-type: none"> 1. The LVJB Board receives reports from both external and internal audit. 2. LVJB has historically not operated an Audit Committee however a new Governance Committee will be introduced from FY18/19. This should provide additional focus on governance, assurance, risk, and compliance issues across the organisation 3. An appropriate structure and membership for this Committee should be established, including a remit in line with Audit Committee good practice, appropriate representation from Board members and specialist input where appropriate. 	Finding 2	<u>Third Line</u> Internal Audit to confirm that the committee has been established with an appropriate term of reference and continues to operate effectively in line with good practice.

Appendix 2 - Basis of our Classifications

Finding rating	Assessment rationale
Critical	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Critical impact on operational performance; or • Critical monetary or financial statement impact; or • Critical breach in laws and regulations that could result in material fines or consequences; or • Critical impact on the reputation or brand of the organisation which could threaten its future viability.
High	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Significant impact on operational performance; or • Significant monetary or financial statement impact; or • Significant breach in laws and regulations resulting in significant fines and consequences; or • Significant impact on the reputation or brand of the organisation.
Medium	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Moderate impact on operational performance; or • Moderate monetary or financial statement impact; or • Moderate breach in laws and regulations resulting in fines and consequences; or • Moderate impact on the reputation or brand of the organisation.
Low	<p>A finding that could have a:</p> <ul style="list-style-type: none"> • Minor impact on the organisation's operational performance; or • Minor monetary or financial statement impact; or • Minor breach in laws and regulations with limited consequences; or • Minor impact on the reputation of the organisation.
Advisory	<p>A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.</p>

Appendix 5 – Terms of Reference

Lothian Valuation Joint Board

Review of LVJB Business Rates Internal Assurance Framework

To: Graeme Strachan, Principal Assessor; Bernie Callaghan, Governance Manager

From: Lesley Newdall, Chief Internal Auditor; Paul McGinty, Principal Audit Manager

Date: 12/02/18

As a result of our discussions with LVJB management it was agreed that the Internal Audit effort for 2017/18 would focus on review of LVJB's current arrangements for internal quality review and checking. Any amendments, revisions or changes to LVJB's underlying data sets or registers are subject to secondary review and checking and this is a fundamentally important aspect of maintaining the underlying integrity of LVJB's registers. The associated internal quality control and checking work is principally undertaken by two members of LVJB staff and management were keen to focus on this area given the wider context of management reviewing overall governance arrangements as part of the Transformation Project and as part of the look forward to 2018/19 where there would be increased focus upon governance.

Scope

It was therefore agreed that our review should include consideration of:

- the overall resourcing and management arrangements in place
- the current focus and targeting of the quality control and checking arrangements
- the processes covered and the robustness of the methodology applied
- the recording and reporting of results
- the follow up and closure of exceptions or management actions.

It was also agreed that our work would consider current arrangements in the wider context of the '3 lines of defence model' and its applicability within LVJB. The Chief Assessor was also keen to ensure some coverage of Records Management arrangements. As such, we will also seek to incorporate a high-level benchmarking review of current arrangements with respect to best practice Records Management.

Approach

Our approach involved:

- Meetings, interviews and inquiries with relevant managers and officers to understand current arrangements
- Assessment of the adequacy of the current arrangements
- Development of a control assessment framework to illustrate how an improved approach could be applied in practice – for this we applied our methodology to the **Business Rates Valuation Roll**
- Highlighting a range of initial recommendations and considerations for management arising from our work
- Highlighting a range of recommendations to support management in the development and ongoing implementation of improved arrangements.

Scope Limitations

Whilst recognising that LVJB provides services to several local authorities, our primary focus was on arrangements as they apply to CEC. At this stage, our work has not involved testing of the operation of

individual controls or procedures in relation to the **Business Rates Valuation Roll**, however this should be a consideration for coverage in subsequent years as well as focus on the risk and control framework applicable to **Council Tax** and **Electoral Register** data sets.

Internal Audit Team

Name	Role	Contact Details
Lesley Newdall	Chief Internal Auditor	Lesley.Newdall@edinburgh.gov.uk
Paul McGinty	Principal Audit Manager	Paul.McGinty@edinburgh.gov.uk

Key Contacts

Name	Title	Role	Contact Details
Bernie Callaghan	Head of Governance	Key Contact	Bernie.Callaghan@lothian-vjb.gov.uk
Nick Chapman	Depute Assessor	Key Contact	nick.chapman@lothian-vjb.gov.uk
Graeme Strachan	Assessor	Review Sponsor	graeme.strachan@lothian-vjb.gov.uk