Pensions Audit Sub-Committee

2pm, Tuesday, 19 June 2023

Lothian Pension Fund - Internal Audit Update - June 2023

Item number 6.4

1. Recommendations

The Pensions Audit Sub-Committee is requested to note:

1.1 Finalisation of the 2022/23 the Lothian Pension Fund internal audit plan, including the outcomes of the recent Information Governance audit;

1.2 Planning for the 2023/24 the Lothian Pension Fund internal audit plan has commenced with an indicative timetable agreed for completing the five audits within the plan;

1.3 Progress with implementation of agreed management actions from previously completed internal audits; and

1.4 The IA annual activity report and opinion which provides an assessment of the overall effectiveness of the Lothian Pension Fund's governance, risk, and control framework for 2022/23 is presented to the Committee for review in a separate paper at this meeting.

Laura Calder
Head of Internal Audit, City of Edinburgh Council

Legal and Assurance, Corporate Services Directorate

E-mail: laura.calder@edinburgh.gov.uk | Tel: 0131 469 3077

2. Executive Summary

2.1 This report provides details of the progress of Internal Audit's (IA) assurance activity on behalf of Lothian Pension Fund (LPF) overseen by the City of Edinburgh Council's (the Council) IA function across the period from 10 February to 1 May.

2.2 The three audits included in the 2023/24 IA annual plan agreed by Committee in September 2022 are now complete.

2.3 A report detailing the outcomes of the Information Governance audit recently completed is included for the Committee's review and scrutiny.

2.4 Planning for the 2023/24 LPF internal audit plan has commenced with an indicative timetable agreed for completing the five audits within the plan.

2.5 As at 27 April 2023, LPF had 28 management actions with 3 actions passed the original implementation date. A total of 8 actions have been closed since February, and 22 new actions raised following completion of audits.

2.6 The IA annual activity report and opinion which provides an assessment of the overall effectiveness of LPFs governance, risk, and control framework for 2022/23 is presented to the Committee for review in a separate paper at this meeting.

3. Background

2022/23 Internal Audit Annual Plan

3.1 The 2022/23 LPF IA plan comprised of three audits following approval from the Pensions Audit Sub Committee in March to defer the Information Security Arrangements audit to the 2023/24 LPF annual IA plan.

3.2 **2023/24 Internal Audit Annual Plan**

The 2023/24 LPF IA plan, which comprises five audits was agreed by the Pensions Audit Sub Committee in March.

Internal Audit Follow-Up Process

3.3 IA follow up on progress with implementation of management actions arising from IA reports. A risk-based approach to follow-up is applied, with all high rated management actions validated by IA when presented for closure together with a sample of medium actions. The remaining medium actions and low actions are closed via a 'self-attestation' once confirmed as complete by management.

4. Main Report

2022/23 LPF IA annual plan

4.1 The 2022/23 IA annual plan included the following reviews:

- Project Forth – Programme assurance (complete December 2022)
- Third-party supplier management (complete March 2023)
- Information governance (complete April 2023)
- Information Security Arrangements

4.2 Following agreement from the Pensions Audit Sub Committee in March 2023, the Information Security Arrangements audit has been deferred to the 2023/24 LPF annual IA plan. Indicative timing is agreed for September 2023, to allow sufficient time to implement associated findings from the recently completed Information Governance audit.

4.3 The Information Governance audit is now complete and a report detailing the outcomes is included at Appendix 1 for review and scrutiny by Committee. The overall assurance rating for this audit is Reasonable Assurance, with a total of 6 findings raised (2 high, 2 medium and 2 low).

4.4 Our review recognises that the new policies and procedures are still being embedded and notes the aspiration to improve the overall information security posture within LPF. Our findings are intended to enhance and strengthen LPF's information governance framework across the following areas:

- implementation and development of key policy, standards, and procedures
- establishing guidance for granting, managing and revoking access to LPF systems and data
- ensuring the recently created data classification and handling standard is cross referenced across other relevant key policies and processes
- establishing clear roles and governance structures for information governance
- monitoring policy compliance
- enhancing the Information Asset Register

2023/24 LPF IA annual plan

4.5 The 2023/24 IA annual plan agreed by Committee in March 2023 includes the five reviews, with proposed timescales for completion of these audits as follows:

Audit	Timescale
People Processes	Q1/Q2 Mid- May to July
Senior Manager Certification Regime	Q2/Q3 Aug to October
Business Continuity and incident response	Q2/Q3 Aug to October

Information Security Arrangements	Q2/Q3 September to December
Project Forth – Targeted review	To be confirmed

Status of Open IA management actions as at 27 April 2023

4.6 As at 27 April 2023, LPF had 28 agreed management actions (8 high, 16 Medium and 4 Low) which were raised across the following audits:

- Bulk Transfers (3)
- Risk Management (2)
- Technology Model Development (1)
- Third Party Supplier Management (7)
- Information Governance (15)

4.7 Three management actions have passed their original implementation date, however revised dates have been provided by management reflecting ongoing actions. Details are included at items 4, 5 and 6 on Appendix 2.

4.8 The remaining 25 management actions are not yet due for completion and implementation is currently being progressed by LPF. Details of the management actions and progress, where relevant are provided at Appendix 2.

5. Financial impact

5.1 Failure to close management actions and address the associated risks in a timely manner may have financial impacts which are not yet measurable.

6. Stakeholder/Regulatory Impact

6.1 IA recommendations are raised when control gaps or deficiencies are identified during audits. If management actions are not implemented, LPF will be exposed to the risks associated with the key processes, including the potential risk of non-compliance with applicable regulations.

7. Background reading/external references

7.1 Public Sector Internal Audit Standards

7.2 Lothian Pension Fund – 2022/23 Internal Audit Annual Plan – September 2022

7.3 Lothian Pension Fund – 2023/24 Internal Audit Annual Plan – March 2023

8. Appendices

Appendix 1	Internal Audit Report - Information Governance
Appendix 2	LPF outstanding audit actions as at 27 April 2023

LOTHIAN
PENSION FUND

EDINBVRGH
THE CITY OF EDINBURGH COUNCIL

Appendix 1

Internal Audit Report

Lothian Pension Fund – Information Governance

5 May 2023

LPF2203

Overall Assessment	**Reasonable Assurance**

Contents

This Internal Audit review is conducted by the City of Edinburgh Council for the Lothian Pension Fund under the auspices of the 2022/23 internal audit plan approved by the Pensions Audit Sub-Committee in September 2022. The review is designed to help the Lothian Pension Fund 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. The City of Edinburgh Council accepts no responsibility for any such reliance and disclaims all liability in relation thereto.

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.

Although there are 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 Lothian Pension Fund. 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 members as appropriate.

Executive Summary

Overall Assessment	Reasonable Assurance

Overall opinion and summary of findings

Lothian Pension Fund (LPF) moved to a new IT provider in 2021 which necessitated the creation for a new Information Governance framework. A suite of new policies and procedures were developed during the last quarter of 2022.

Our review recognises that the new policies and procedures are still being embedded and notes the aspiration to improve the overall information security posture within LPF. Our findings are intended to enhance and strengthen LPF's information governance framework.

- **Policy, Standards & Procedures implementation –** numerous policies and procedures are currently in draft state or yet to be created. A further six documents that are currently not planned to be created but which would contribute to effective information governance were also identified. Additionally, LPF has not established a process or mechanism to update and manage all the policies and procedures centrally.
- **Access management –** LPF do not have dedicated policies and procedures for controlling access to data, with an overall absence of guidance around the process for how access should be granted, managed, and removed for LPF systems and data.
- **Data classifications** – whilst a new data classification policy was recently created (Data Classification and Handling Standard), data classifications have not yet been referenced in other policies.
- **Information governance structure** – LPF does not currently have an overarching governance forum that is responsible for oversight of Information Governance and provides a regular touchpoint with the City of Edinburgh Council's Data Protection Officer. Additionally, both data and system owners within LPF are called Information Asset Owners creating potential confusion regarding roles & responsibilities.
- **Compliance monitoring –** whilst LPF has a compliance monitoring plan in place, the majority of information governance related policies are not featured within the plan. Consequently, there is minimal monitoring over compliance, including breaches of policies.
- **Information Asset register -** the Information Asset register is not sufficiently detailed. It has not combined the Third-party Systems list and does not overlay the current Retention Schedule across it, to enable a holistic view over LPF's data.

Areas of good practice

- The Information Governance Policy acts as a 'directory', coordinating all information governance policies, procedures, and their respective activities
- Information Governance policies and procedures are centrally stored within LPF's SharePoint and available to all LPF members, with these documents communicated across LPF via email, face to face training, all colleague calls, and the annual declaration form.

Management response

As described in the background section, a number of assurance and uplift activities have been undertaken since 2021, including an Information Governance project where refreshed policies and procedures were agreed with CEC's Information Governance Unit, and a formal Information Security project. Du e to unforeseen events during Q4 2022 and Q1 2023, implementation and planned improvements – including access and change management, data classification, compliance monitoring – have been delayed. LPF will incorporate the identified recommendations into the rebased project activities, which will ensure a co-ordinated and robust approach to Information Governance and Information Security arrangements across LPF.

Audit Assessment

Audit Area	Control Design	Control Operation	Findings	Priority Rating
1. Policies and Procedures	🟠	🔴	Finding 1: Policy, standards & procedures implementation	High Priority
2. Data classification and ownership	🔴	N/A	Finding 2: Access management	High Priority
3. Data Classification and Ownership	🔴	N/A	Finding 3: Data classifications	Medium Priority
4. Governance	🟠	N/A	Finding 4: Information governance structure	Medium Priority
5. Compliance Monitoring	🟠	N/A	Finding 5: Level of compliance monitoring	Low Priority
6. Data Classification and Ownership	🟠	🟢	Finding 6: Information Asset register	Low Priority

See Appendix 1 for Control Assessment and Assurance Definitions

Background and scope

Lothian Pension Fund (acting through its administering authority the City of Edinburgh Council (the Council)) is a local government pension fund in Scotland with over 80,000 members and c.90 employers. LPF holds data about its members and their next of kin which allows it to perform core functions such as collecting pension contributions and paying pension benefits.

Therefore, it is key for the LPF to ensure that the information and data it holds is well managed, appropriately classified, utilised for maximum benefit across pension scheme where possible and retained in line with relevant compliance requirements, which is enabled by good governance around the management and use of data. Being the data processor and operating in a regulated environment, it is necessary for LPF to understand the value of their data to ensure it is managed securely.

LPF moved to a new IT provider in 2021 and previously followed the Council's information Governance framework. At the point of transferring to the new provider they could no longer access the Council's policy and procedures and therefore set out to create their own Information governance framework and data related policies, with the aim of completing them by end of 2022. An information security project was commenced, with an external consultant engaged to audit LPF against the NIST (National Institute of Standards and Technology) security framework and a project plan created to remediate the findings of this audit

Whilst LPF own the contract with their incumbent IT provider, the Council are considered as the data controller. The new framework and data policies have been developed alongside the Council but tailored to meet LPF's standards and requirements.

Scope

The objective of this review was to assess the adequacy of design effectiveness of the key controls established to ensure LPF's controls over data strategy and information governance.

This included consideration of key controls over strategy and governance including how the roles and responsibilities of LPF stakeholders fit together to ensure that the data is well managed. The review also considered data classification and ownership, and data content management.

Risks

The review also assessed the following LPF risks:

- Data protection
- Information Rights

Limitations of Scope

Internal audit testing was performed on a sample basis with a focus on key controls mitigating risks.

Testing was designed to assess the adequacy and effectiveness of key controls in operation during 2022/23.

Work on data protection was limited to understanding what steps LPF have adopted to ensure compliance with the data protection process and does not represent a compliance audit.

Reporting Date

Testing was undertaken between 6 February 2023 and 10 March 2023.

Our audit work concluded on 10 March 2023, and our findings and opinion are based on the conclusion of our work as at that date.

Findings and Management Action Plan

Finding 1 – Policy, Standards & Procedures Implementation

Finding Rating	High Priority

Formal policies, standards, and procedures covering all activities across the entire information lifecycle should be in place. These should align with relevant regulation and standards, including any applicable from regulators such as Pensions Regulator or the Information Commissioner's Office (ICO), and be subject to regular review and update.

LPF are currently in the process of redesigning their wider information governance approach and, due to unexpected circumstances, this project is behind schedule. However, the following issues were observed during this review:

1. The following f documents which would support effective information governance within LPF have not been created and management have advised there is no current plan to create them:
   - Matrix on roles (RACI) to execute the current deliverables
   - Data Strategy
   - Data Archiving policy
   - Information Governance Control Framework
2. Of the forty five policies featured in LPF's ISMS (information security management system) document tracker, there are sixteen policy, standard and procedure documents relating to information governance that are not yet created or are still in draft (see Appendix 2). Additionally, no formal roadmap to create and implement these policies exists.
3. Whilst policies have formal review dates and version control, there is no centralised monitoring and management of these policies to ensure policies are subject to regular review and updates in line with review dates.

Risks

Data protection/ Information Rights

- absence of key policies may result in lack of understanding for key processes and result in a potential breach of operational and information security standards.

Recommendations and Management Action Plan: Policy, Standards & Procedures Implementation

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officer	Timeframe
1.1	Management should consider whether the following policies noted as absent are required for LPF: • Matrix on roles (RACI) to execute the current deliverables • Data Strategy • Data Archiving policy	Ownership of deliverables will be document as part of 1.2 action, for Information Security Project. LPF will incorporate data strategy, data archiving, and information governance	Chief Executive Officer (LPF)	Chief Risk Officer	RACI: 30/06/2023 Others: 31/12/2023

	- Information Governance Control Framework	controls into new or existing documentation.			
1.2	LPF should create a roadmap, covering the development and implementation of the policies required. The roadmap should include set milestone dates for creating and/or releasing with assigned owners responsible for delivery.	LPF's existing Information Security project is being rebased, and the new project will specify plans for delivery of remaining policies / artifacts - including dates and owners.	Chief Executive Officer (LPF)	Head of IT	30/06/2023
1.3	LPF should implement a clearly defined process to ensure a centralised management of policies and procedures to ensure policies are reviewed at a defined timescale and in collaboration with relevant stakeholders.	LPF will implement a group-wide approach for centralised management of policies and procedures.	Chief Executive Officer (LPF)	Chief Risk Officer	31/12/2023

Finding 2 – Access management

Finding Rating	High Priority

Robust access management control procedures and policies preserve the integrity of the IT environment, ensuring that only appropriate users are granted access to systems and data.

LPF do not currently possess dedicated policies and procedures for controlling access to systems and data. There is an overall lack of guidance around the process for how access should be granted, managed, and removed to LPF systems and data. Our review noted the following issues with access management:

1. A formal Joiners, movers, leavers policy has not been developed. In addition, there is no formal process in place to ensure that leavers access to systems and data is revoked on a timely basis.
2. An identity and access management policy is currently in draft. However, it does not include a detailed process for how access should be granted, reviewed, and removed as required.
3. LPF's current access management policies do not detail what additional procedures and controls should be applied when third parties and/or contractors are accessing LPF's data.

Risks

Data protection / Information Rights

- data may not be restricted to appropriate individuals resulting in unauthorised access and/or data leakages leading an increased risk of data breaches.
- key data required to enable officers to undertake their roles may not be accessible resulting in a negative impact on operational performance.

Recommendations and Management Action Plan: Access Management

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officer	Timeframe
2.1	LPF should create and implement a formal Joiners, Movers, Leaver's policy. This should focus on processes to ensure access to applications are granted and removed in a timely manner, providing prescriptive procedures for LPF staff to follow. The policy should include implementation of a regular quality check to review movers and leavers and ensure access rights remain appropriate and access has been revoked where relevant. This policy should be delivered as part of the policy roadmap at recommendation 1.2.	LPF's existing approach to Joiner Movers Leavers will be documented. Documentation of access rights and processes will be co-ordinated across JML and new Change & Access policies and procedures.	Chief Executive Officer (LPF)	Chief People Officer	31/12/2023

2.2	LPF should update the draft access control procedure to include a detailed process for granting and managing access to LPF users and applying any additional controls for granting access to external parties (where applicable)	LPF's draft Change Management and Identity and Access policies will be updated to cover granting, management, and removal of users. Measures re external party access will also be documented.	Chief Executive Officer (LPF)	Head of IT	31/12/2023

Finding 3 – Data classifications

Finding Rating	Medium Priority

Effective and accurate classification of data is critical to ensuring that the nature and contents of the data is understood and clearly visible within the organisation, enabling appropriate management activities to be undertaken and compliance with applicable guidelines (i.e., GDPR, Government security classifications, pension regulator) maintained.

Our review noted that LPF does not use data classifications to inform the management & governance activities they undertake over the data. The following issues were observed:

1. Whilst a new data classification policy was recently created, data classifications have not yet been referenced in other documentation where it would be expected that data classifications are a factor in dictating how types of data should be handled. These documents include but are not limited to:
   - Data Retention Schedule
   - Information Asset Register
   - Data Breach Policy
2. The data classification policy does not acknowledge special categories or sensitive data, with all personal data covered under a single classification (Personal confidential) and no distinguishment made between the different types of personal data held by LPF.
3. Record retention periods are currently determined independently of data classification, this being a consequence of LPF having not yet updated the record retention periods they inherited from the Council. Additionally, whilst a record retention schedule exists and is utilised, no document providing higher-level guidance and principles on determining what records should be retained for a certain period exists.

Risks

Data protection / Information Rights

- inadequately classified data may lead to inconsistencies in requirements for capturing, processing, storing and retention and the same type of data potentially being treated different across the organisation; and
- business units may not have identified all data protection risks, leading to potential non-compliance and financial penalties and reputational damage.

Recommendations and Management Action Plan: Data classifications

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officer	Timeframe
3.1	LPF should perform a review to identify which policies should reference and apply the data classifications policy. For policies where this applies, the policy should be updated so data classification directly determines the management and governance activities that are undertaken. This recommendation should be implemented once recommendations 1.1 and 1.2 are completed, so a	As part of LPF's planned data classification implementation, existing documents will be reviewed to ensure they reference, and align with, data classification approach.	Chief Executive Officer	Chief Risk Officer	31/12/2023

	complete suite of policies is available for review and updating.				
3.2	LPF should update the data classification policy, to ensure it explicitly identifies the different categories of personal data in accordance with GDPR guidelines, including special categories. The policy should also provide a clear definition of a ‘data asset’ and align the policies to this definition as a baseline.	LPF will update data classification policy to specify approach to special category data. LPF will define ‘data asset’ and align policies to this definition.	Chief Executive Officer	Head of IT	31/12/2023
3.3	LPF should update the retention schedule, so a data asset’s classification influences the asset’s retention period. Alongside this, LPF develop a high-level document which provides guidance on how the data retention periods should be determined in relation to data classification.	LPF will: 1. create documented guidance on how retention periods are determined, including how CEC’s requirements are tailored to LPF. 2. update retention schedule to align with LPF's data assets	Chief Executive Officer	Chief Risk Officer	31/12/2023

Finding 4 – Information governance structure

Finding Rating	Medium Priority

A dedicated, robust governance structure is essential to sustain good information governance, providing key stakeholders with adequate and appropriate visibility and oversight regarding data and information governance. Clearly assigned ownership of data assets within this structure is critical to ensuring effective maintenance and compliance with organisation policies and standard occurs.

Review of LPF's current information governance structure highlighted:

1. There is no overarching governance forum that represents the central management function and authority regarding information governance. This may be covered in other forums (Risk Management Group and IT Oversight Change Group (ITOCG)) however these forums do not include specific roles in relation to information governance within their Terms of Reference.
2. Dedicated reporting on information governance is not provided to stakeholders, both within LPF and the Council, reducing the ability for stakeholders to influence decisions around information governance.
3. No central document summarising all information governance stakeholders within LPF (RACI Matrix) exists, with this information currently spread over multiple different sources.
4. Within documentation both data and system owners within LPF are called Information Asset Owners (IAOs). Consequently, there is lack of clarity regarding which specific individual is being referred to when the IAO title is mentioned, creating potential confusion regarding responsibilities.

Risks

Data protection / Information Rights

- absence of a formally established governance structure for information governance may result in uninformed decision making, services not being delivered in line with expectations and performance improvement opportunities being missed;
- lack of clarity on the IAO designation leading to uncertainty and increased likelihood that information assets may be governed incorrectly.

Recommendations and Management Action Plan: Information governance structure

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officer	Timeframe
4.1	LPF should consider establishing a regular governance forum which has ultimate responsibility for information governance. Alternatively, the Terms of Reference for existing forums (Risk management Group, ITOCG) could be amended to include sufficiently detailed responsibility for information governance.	LPF will assign responsibility for information governance to a governance forum.	Chief Executive Officer	Chief Risk Officer	31/12/2023

4.2	LPF should create a RACI Matrix covering all information governance stakeholders within LPF. The Council's Data Protection Officer (DPO) should also be included in this Matrix.	LPF's information governance policy currently details roles & responsibilities (including CEC's DPO) but not in a RACI format. This will be updated with a clear RACI matrix.	Chief Executive Officer	Chief Risk Officer	31/12/2023
4.3	LPF should review the 'IAO' title so that system and data owners have different titles, allowing them to be easily distinguished from each other within documentation.	LPF will review the use of IAO title and establish a clear definition and use.	Chief Executive Officer	Head of IT	31/12/2023

Finding 5 – Compliance monitoring

Finding Rating	Medium Priority

Formal compliance monitoring and associated reporting enables an organisation to oversee policy implementation and track various processes, such as data retention, disposal, and security to ensure they are being implemented effectively.

The following issues were noted during our review:

1. Minimal monitoring of policy implementation and compliance, including breaches of policies, is undertaken within LPF. LPF have a compliance monitoring plan with quarterly monitoring performed, but this does not cover numerous information governance policies, including:
    - Data protection
    - Record Retention
    - Data Classification
    - Information rights
2. There is no formal approach within LPF for monitoring of data security, resulting in a lack of assurance over whether data is stored appropriately and in compliance with relevant policies & procedures.

Risks

Data protection / Information Rights

- management may be unaware of non-compliance with agreed data security and storage requirements resulting in errors or malpractice and an increased risk of data breaches being undetected
- lack of clarity regarding what data/information is held, captured, and stored and how long it should be retained for. There will be an associated risk if there are changes to the business.

Recommendations and Management Action Plan: Compliance monitoring

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officer	Timeframe
5.1	LPF should implement centralised compliance monitoring of key information governance policies and procedures within LPF, focusing on ensuring they are being correctly followed and any breaches or non-compliance are identified and reported. This may potentially be performed through the LPF Compliance Monitoring Plan, which does not currently cover information governance within its' scope.	LPF will incorporate information governance measures into existing compliance monitoring plan.	Chief Executive Officer	Chief Risk Officer	31/12/2023

5.2	LPF should implement a formal approach by which to monitor information security, focusing on ensuring that data is stored in-line with security requirements detailed in the relevant policies.	LPF will formalise and document the current approach to monitoring information security e.g., regular IT security checks of information security at third parties.	Chief Executive Officer	Head of IT	31/12/2023

Finding 6 – Information Asset register

Finding Rating	Low Priority

Data assets should map across and be consistent between documentation, providing one consistent version of the enabling data assets to be easily identified. The business application owner should know the type of data an application holds to ensure it is stored securely and retained accordingly, where this information is maintained.

The following issues regarding data assets were identified:

1. The Information Asset Register, Record Retention Schedule, and Third-Party Systems List do not coordinate with the list of data assets and systems within LPF:
   - The Information Asset Register only mentions 10 systems out of the 146 on the Third-Party Systems List, resulting in a lack of clarity of what data various systems store and their data classification.
   - The Information Asset Register, which is high level, only lists 8 information assets and these assets are not clearly identifiable in the record retention schedule.
2. Neither the 'Information Asset Owner Role Guidance' or the 'Data Classification and Handling Standard' clarify who is responsible for ensuring the systems information assets are stored on are themselves appropriately secure.
3. Additionally, LPF do not have a formally documented definition of a data asset. Management advised that this is because LPF is a small company, therefore there is implicit knowledge within the organisation of what the data assets are.

Risks

Data protection / Information Rights

- lack of clarity on information assets and how they map across the various systems, leading to uncertainty as to who holds specific data assets, potentially resulting in data being held in systems that LPF is unaware of.
- business units may not have identified all data protection risks, leading to potential non-compliance and financial penalties and reputational damage.

Recommendations and Management Action Plan: Information Asset register review and update

Ref.	Recommendation	Agreed Management Action	Owner	Lead Officer	Timeframe
6.1	The information asset register should be updated by LPF to be a complete record of all data assets within LPF including whether it resides with a third-party supplier. This register should also include a description on the type of data it holds and its retention period.	LPF will review and update its information asset register, and ensure the asset register, system list, third party supplier list, and retention schedule align.	Chief Executive Officer	Head of IT	31/12/2023
6.2	LPF should create and implement a matrix of dependencies for all systems within LPF. This should capture an overview of the systems, key technical	LPF will update existing registers (which may include third party supplier list, system lists, refreshed information asset	Chief Executive Officer	Head of IT	31/12/2023

	details (version, hosting, etc.), the data within them and where potential risks exist and what data is impacted by these risks.	register) to capture details; and create overview diagram(s) to illustrate the flow of business-critical systems.			

Appendix 1 – Control Assessment and Assurance Definitions

Control Assessment Rating		Control Design Adequacy	Control Operation Effectiveness
Well managed	🟢	Well-structured design efficiently achieves fit-for purpose control objectives	Controls consistently applied and operating at optimum level of effectiveness.
Generally Satisfactory	🟢	Sound design achieves control objectives	Controls consistently applied
Some Improvement Opportunity	🟡	Design is generally sound, with some opportunity to introduce control improvements	Conformance generally sound, with some opportunity to enhance level of conformance
Major Improvement Opportunity	🔴	Design is not optimum and may put control objectives at risk	Non-conformance may put control objectives at risk
Control Not Tested	**N/A**	Not applicable for control design assessments	Control not tested, either due to ineffective design or due to design only audit

Overall Assurance Ratings	
Substantial Assurance	A sound system of governance, risk management and control exist, with internal controls operating effectively and being consistently applied to support the achievement of objectives in the area audited.
Reasonable Assurance	There is a generally sound system of governance, risk management and control in place. Some issues, non-compliance or scope for improvement were identified which may put at risk the achievement of objectives in the area audited.
Limited Assurance	Significant gaps, weaknesses or non-compliance were identified. Improvement is required to the system of governance, risk management and control to effectively manage risks to the achievement of objectives in the area audited.
No Assurance	Immediate action is required to address fundamental gaps, weaknesses or non-compliance identified. The system of governance, risk management and control are inadequate to effectively manage risks to the achievement of objectives in the area audited.

Finding Priority Ratings	
Advisory	A finding that does not have a risk impact but has been raised to highlight areas of inefficiencies or good practice.
Low Priority	An issue that results in a small impact to the achievement of objectives in the area audited.
Medium Priority	An issue that results in a moderate impact to the achievement of objectives in the area audited.
High Priority	An issue that results in a severe impact to the achievement of objectives in the area audited.
Critical Priority	An issue that results in a critical impact to the achievement of objectives in the area audited. The issue needs to be resolved as a matter of urgency.

Appendix 2 – ISMS Document Tracker

Document Title	Status	Relevant for information governance
Third Party Security Assurance Standard	Not created	Y
Business Continuity Test Procedure	Not created	N
Phishing and Penetration Test Schedule	Not created	N
Business Continuity and Recovery Policy	Not created	N
LPF Incident Management Process	Not created	Y
Business Continuity Report Template	Not created	N
Physical and Environmental Security Policy	Not created	N
Risk Assessment and Treatment Methodology	Not created	Y
Controls Exception Log	Not created	N
Password Policy	Not created	Y
Supply Chain Security Standard	Not created	N
Asset Management Standard	Draft	N
Backup Policy	Draft	Y
Bring Your Own Device (BYOD) Policy	Draft	N
Bring Your Own Device (BYOD) Standard	Draft	N
Call Recording Policy	Draft	N
Change Management Policy	Draft	N
Change Management Process Starter	Draft	N
Cryptographic Policy	Draft	Y
Cryptography Standard	Draft	Y
Access Control Procedure	Draft	Y
Identity and Access Management Policy	Draft	Y
Identity and Access Management Standard	Draft	Y
Information Transfer Policy	Draft	Y

Logging and Monitoring Policy	Draft	N
Logging and Monitoring Standard	Draft	N
Information Security Communications Plan	Draft	N
Information Security Context, Requirements and Scope	Draft	N
Information Security Policy	Draft	N
ISMS Monitoring and Measurement	Draft	N
Management of Non-conformance and Corrective Action Policy	Draft	Y
Nonconformity and Corrective Action Log	Draft	N
Network Security Policy	Draft	N
Information Security Risk Management Policy	Draft	Y
Information Security Risk Management Standard	Draft	Y
Vulnerability and Patch Management Policy	Draft	Y
Vulnerability and Patch Management Standard	Draft	Y
Clear Screen and Clear Desk Policy	Live	Y
Security Incident Response Plan	Live	N
Data Classification and Handling Standard (LGSC)	Live	Y
Media Handling Policy	Live	N
IT Operational Risk Log	Live	Y
Acceptable Use Policy	Live	Y
Business Continuity Plan	Live	N
Information Asset Owner Role	Live	Y

Appendix 2 - LPF Internal Audit Management Actions as at 27 April 2023

Ref	Audit	Audit progress	Rec Title	Agreed Management Action	Rating	Status	Est Date	Revised Date	Management Update
1	**LPF2001 Bulk Transfers**	**25%** 4 actions 1 complete 3 outstanding **0 overdue**	Rec 2.1 Maintenance and oversight of a data transfer issues log	A data transfer issues log will be created for data transfer exercises, the log will be reviewed and verified by an independent officer, and a quality assurance process to review a sample of issues implemented.	Medium	**Not yet due**	31/12/2024	n/a	Not yet due
2			2.2 Completion of parallel payroll runs	A formal process will be established to confirm satisfactory completion of the payroll run and to ensure that issues are identifed and recorded in the issue log.	Medium	**Not yet due**	31/12/2024	n/a	
3			2.3 Review of membership communication listing	Processes to support future communications to members re transfer will be formalised in line with the recommendation including reconciliation and review to confirm accuracy.	Medium	**Not yet due**	31/12/2024	n/a	
4	**LPF2003 Technology Model Development**	**86%** 7 actions 6 complete 1 outstanding **1 overdue**	3.1.2: Post-Implementation Activities - User manuals	LPF have produced user manuals and documentation for key/business critical systems and will review the requirements and suitability of the currently available generic documentation for the other third party systems.	Medium	**Overdue (revised date)**	31/12/2022	31/12/2023	The following action has been taken - establishing and refreshing full population of LPF systems, and requesting system owners create system manuals which has identified that a wider review and categorisation of systems by criticality is required, to allow a proportionate approach. E.g. ensuring that critical operational systems have user manuals; while less critical systems (such as information portals) require less comprehensive documentation. Date changed to Dec 2023, to allow this to be co-ordinated with other existing projects (IT and Supplier Management).
5	**LPF2103 Risk Management**	**33%** 3 actions 1 complete 2 outstanding **2 overdue**	1.1 Aligning corporate risks with strategic objectives and risk definitions	Risks will be reviewed with this finding in mind and use it as an opportunity to step back and consider more holistically the risks we capture and how we can effectively manage and cascade granularity of definition with both ongoing operational risk management and reporting/governance. The Risk Management Group (RMG) does seek to do this on an ongoing basis, and to strike the important balance between maintaining and reporting on the right number of risks (omitting gaps) and distracting the focus away from critical risks/strategic analysis with too much detail, but this is a helpful and timely point to review this. We will consider within RMG and report back through the usual channels with any updates arising.	Medium	**Overdue (revised date)**	31/03/2023	31/12/2023	A wider review and uplift of LPF's Risk Management Framework is underway and the observations made by Internal Audit will be integrated into this review.
6			2.1 Maintenance of risk registers	We will look to re-review the sub-group registers (and tie-in with main group register) with these points in mind We will consider within Risk Management Group (RMG) and report back through the usual channels with any updates arising.	Low	**Overdue (revised date)**	31/03/2023	31/12/2023	
7	**LPF2203 Third Party Supplier Management**	**0%** 7 actions 0 complete 7 outstanding **0 overdue**	1.1 Business Case Documentation for critical suppliers	LPF will review records for existing critical suppliers and ensure that business case documentation is stored in correct supplier files. Supplier management policy will be updated to specify where supplier records, such as business case, should be stored.	High	Not yet due	30/09/2023		Not applicable - NEW
8			1.2 and 1.3 Training for Tier 1 supplier owners / due diligence	1.2 LPF will carry out targeted training for Tier 1 supplier owners on monitoring and consider appropriate oversight via RMG reporting. 1.3 As part of action 1.2, targeted training will cover annual due diligence. Supplier framework document review will consider due diligence templates or checklists with set items, tailored to specific tiers.	High	Not yet due	30/06/2023		Not applicable - NEW

Ref	Audit	Audit progress	Rec Title	Agreed Management Action	Rating	Status	Est Date	Revised Date	Management Update
9			1.5 Communication of incident reporting processes to employees	LPF will recommunicate existing incident reporting policies to all employees.	High	Not yet due	30/09/2023		Not applicable - NEW
10			3.1 Review of supplier management framework	LPF will review existing Supplier Management Framework document and all related supporting document (templates, checklists), and update. New supporting documents will be created where necessary . **This will cover Recs 1.4, 2.1, 2.2, 4.1, 4.2, 4.3 and 5.2**	Medium	Not yet due	31/12/2023		Not applicable - NEW
11			5.1 Enhancements to and review of supplier database	LPF will enhance existing supplier database to include additional data fields, including dates of IT assessment and DPIA, and links to full records. A review of the database will be established, with results provided to senior management as part of RMG oversight.	Medium	Not yet due	30/09/2023		Not applicable - NEW
12			5.3 Risk Management Group (RMG) responsibilties	LPF will update RMG responsibilities to include supplier management, and consider how best to incorporate into existing agenda and MI. LPF will add document control to RMG Terms of Ref, including version history and frequency of review.	Medium	Not yet due	30/06/2023		Not applicable - NEW
13			6.1 Supplier management training and awareness	LPF will carry out training and awareness following update of all documents and processes referred to in other actions; and consider how to incorporate into existing annual training plan and onboarding.	Low	Not yet due	31/12/2023		Not applicable - NEW
14	**LPF2202 Information Governance**	**0%** 15 actions 0 complete 15 outstanding **0 overdue**	1.1 - Policy, Standards & Procedures Implementation	LPF will incorporate data strategy, data archiving, and information governance controls into new or existing documentation. RACI will be covered at 4.2.	High	Not yet due	31/12/2023		Not applicable - NEW
15			1.2 - Roadmap for remaining policies/artifacts	LPF's existing Information Security project is being rebased, and the new project will specify plans for delivery of remaining policies / artifacts - including dates and owners.	High	Not yet due	30/06/2023		Not applicable - NEW
16			1.3 - Centralised management of policies and procedures	LPF will implement a group-wide approach for centralised management of policies and procedures.	High	Not yet due	31/12/2023		Not applicable - NEW

Ref	Audit	Audit progress	Rec Title	Agreed Management Action	Rating	Status	Est Date	Revised Date	Management Update
17			2.1 - Documented Access Management Approach	LPF's existing approach to Joiner Movers Leavers will be documented. Documentation of access rights and processes will be co-ordinated across JML and new Change & Access policies and procedures.	High	Not yet due	31/12/2023		Not applicable - NEW
18			2.2 - Access Management for external parties	LPF's draft Change Management and Identity and Access policies will be updated to cover granting, management, and removal of users. Measures re external party access will also be documented.	High	Not yet due	31/12/2023		Not applicable - NEW
19			3.1 - Review of existing documents and data classification	As part of LPF's planned data classification implementation, existing documents will be reviewed to ensure they reference, and align with, data classification approach.	Medium	Not yet due	31/12/2023		Not applicable - NEW
20			3.2 - Update of Data Classification policy to include special category data and define data asset	LPF will update data classification policy to specify approach to special category data, will define 'data asset' and align policies to this definition.	Medium	Not yet due	31/12/2023		Not applicable - NEW
21			3.3 - Retention schedule guidance	LPF will: 1. create documented guidance on how retention periods are determined, including how CEC's requirements are tailored to LPF. 2. update retention schedule to align with LPF's data assets	Medium	Not yet due	31/12/2023		Not applicable - NEW
22			4.1 - Information governance forum	LPF will assign responsibility for information governance to a governance forum.	Medium	Not yet due	31/12/2023		Not applicable - NEW
23			4.2 - Information governance roles and responsibilities (RACI)	LPF's information governance policy currently details roles & responsibilities (including CEC's DPO) but not in a RACI format. This will be updated with a clear RACI matrix.	Medium	Not yet due	31/12/2023		Not applicable - NEW
24			4.3 - Review of IAO title	LPF will review the use of IAO title and establish a clear definition and use.	Medium	Not yet due	31/12/2023		Not applicable - NEW
25			5.1 - Compliance Monitoring	LPF will incorporate information governance measures into existing compliance monitoring plan.	Medium	Not yet due	31/12/2023		Not applicable - NEW

Ref	Audit	Audit progress	Rec Title	Agreed Management Action	Rating	Status	Est Date	Revised Date	Management Update
26			5.2 - Formalising information security monitoring approach	LPF will formalise and document the current approach to monitoring information security e.g., regular IT security checks of information security at third parties.	Medium	Not yet due	31/12/2023		Not applicable - NEW
27			6.1 - Information Asset register review and update	LPF will review and update its information asset register, and ensure the asset register, system list, third party supplier list, and retention schedule align.	Low	Not yet due	31/12/2023		Not applicable - NEW
28			6.2 - Update of registers to illustrate system dependencies	LPF will update existing registers (which may include third party supplier list, system lists, refreshed information asset register) to capture details; and create overview diagram(s) to illustrate the flow of business-critical systems.	Low	Not yet due	31/12/2023		Not applicable - NEW