Paisley
Housing Association

Paisley HA & Paisley South Property Services Group Policy

Risk Management Policy

Policy on:	Risk Management

Compliant with Charter:	2: Equalities 14. Rent and Service Charges
Compliant with New Regulatory Framework:	Regulatory Standards of Governance and Financial Management Standard 3: The RSL manages its resources to ensure its financial well-being, while maintaining rents at a level that tenants can afford to pay. Standard 4: The governing body bases its decisions on good quality information and advice and identifies and mitigates risks to the organisation's purpose
Compliant with Tenant Participation Strategy:	N/A
Compliant with Equalities and Diversity Policy	YES
Compliant with Business Plan:	Building Organisational Resilience

Date of Approval: Date for next review:	By the Full Board August 2024 May 2029

Responsible Officer:	Head of Finance & IT, Lorna Colville

<u>**INDEX**</u>

1. PURPOSE OF THIS DOCUMENT

This Risk Management Policy (the Policy) is a group policy and must be complied with by both Paisley Housing Association and Paisley South Property Services (PHA & PSPS). It forms part of our internal control and corporate governance arrangements.

PHA recognises that effective risk management is essential for achieving our strategic objectives while safeguarding our reputation, financial stability, and long-term sustainability.

This policy outlines**:**

- our commitment to proactive risk identification, assessment, mitigation, and continuous improvement.
- the roles and responsibilities of the governing body, the Group Audit & Risk Committee, the senior management team and staff. It
- the key aspects of the risk management process and identifies the main reporting procedures

In addition, it describes the process the governing body (i.e. the Board) will use to evaluate the effectiveness of the organisation's internal control procedures.

2. WHY WE NEED TO MANAGE RISK?

The focus on risk management is as part of the process to ensure effective governance, sound business planning & financial management, safeguarding stakeholder assets and delivering **good** outcomes for tenants & other Service Users

The Scottish Housing Regulator's Regulatory Standards of Governance and Financial Management (2024)

- Standard 3.3 states: The RSL has a robust business planning and control framework and effective systems to monitor and accurately report delivery of its plans. Risks to the delivery of financial plans are identified and managed effectively. The RSL considers sufficiently the financial implications of risks to the delivery of plans.
- Standard 4.4 states: The governing body identifies risks that might prevent it from achieving the RSL's purpose and has effective strategies and systems for risk management and mitigation, internal control and audit.

PHA also publishes annual a 'Statement on Internal Financial Control' approved by the Board and included in the financial statements of PHA. An effective Risk Management Policy is an integral part of this assurance and is crucial to support the statement. PHA & PSPS will continue to focus on embedding risk management throughout the organisation by putting in place a pro-active risk management framework

Risk Management is beneficial to the group as it:

- helps us to be more flexible and responsive to new internal / external demands.
- helps PHA & PSPS make informed decisions.

- provides assurance to the governing body, the Group Audit & Risk Committee and the PHA Senior Management Team.
- reduces incidents and other control failures; and
- helps in the achievement of PHA & PSPS 's key targets and priorities

Managing the risks to our business objectives reduces the chance of us having to deal with the unexpected and ensures proactive management rather than reactive crisis management. At a time when resources are limited it is especially important to reduce the number of unwanted surprises.

The framework for managing risk sets out the process through which risks will be identified, assessed, controlled, monitored and reviewed. The framework is designed to:

- Integrate risk management into the culture of PHA & PSPS.
- Raise awareness of the need for risk management.
- Encourage a positive approach to risk management.
- Support improved decision making, innovation and performance, through a good understanding of risks and their likely impact; and
- Manage risk in accordance with best practice.

3. DEFINITIONS

What is a risk?

“The threat or possibility that an action or event will adversely affect an organisation’s ability to achieve its objectives or a business opportunity”.

What is risk management?

“Risk Management is the process which aims to help PHA & PSPS understand, evaluate and take action on all our risks with a view to increasing the probability of our success and reducing the likelihood of failure”.

4. RISK MANAGEMENT AIMS AND OBJECTIVES

- We provide continuous high-quality services to the tenants & other customers of PHA & PSPS.
- We adopt a Group wide approach to risk management that considers risks across all aspects of the Group, including operations, finance, compliance, reputation, and strategy. This holistic approach of risk management ensures that risks are identified, assessed, and managed in a coordinated manner, considering both internal and external factors.
- Our Board, Audit & Risk Committee and Senior Management Team play a pivotal role in risk oversight. They ensure the integration of risk management into strategic decision-making, challenge assumptions, and set the risk appetite.
- We foster a strong risk-aware culture throughout the Group where risk management is embedded into decision-making processes and the everyday working situations of all staff. We encourage open communication about risks and empower employees at all levels to identify and escalate concerns.
- We use appropriate identification and analysis techniques to identify risks to PHA & PSPS and determine the long and short-term impact.

- We prioritise and implement economic control measures to reduce or remove risks.
- We plan to improve Crisis preparedness and response plans in those areas considered High Risk and ensure these are regularly reviewed and tested.
- We protect and promote the reputation of the group.
- Using training and communication, develop and maintain a structured risk management culture.
- Maintain a system for recording and providing accurate, relevant and timely risk management information.
- Reduce the long-term cost of risk to the group.
- Report on and review the Risk Management Policy in accordance with best practice guidelines.

5. UNDERLYING APPROACH TO RISK MANAGEMENT

The following key principles underlie the group's approach to risk management and internal control:

- The governing bodies have responsibility for overseeing risk management within PHA & PSPS relevant to their organisation.
- An open and receptive approach to solving risk problems is adopted by the Board.
- The PHA Chief Executive and Senior Management Team support, advise on and implement policies approved by the Boards.
- Risk management forms part of PHA & PSPS 's system of internal control.
- PHA & PSPS make conservative and prudent recognition and disclosure of the financial and non-financial implications of risks.
- All staff are responsible for encouraging good risk management practices within their areas of responsibility.

6. ROLES AND RESPONSIBILITIES - BOARD

ROLE OF THE GOVERNING BODY

The governing body of PHA has a fundamental role to play in the management of risk.
Their role is to:

- Set the tone and influence the culture of risk management within PHA & PSPS.
  This includes:
  - determining whether PHA & PSPS is 'risk taking' or 'risk averse' as a whole or on any relevant individual issue
  - determining what categories of risk are acceptable and which are not
  - setting the standards and expectations of staff with respect to conduct and probity.
- To approve the regular review of this Risk Management Policy.
- Determine the appropriate risk appetite or level of exposure for PHA & PSPS.
- Approve major decisions affecting PHA & PSPS's risk profile or exposure.
- Monitor the management of significant risks to reduce the likelihood of unwelcome surprises.
- Satisfy itself that the less significant risks are being actively managed, with the appropriate controls in place and working effectively.

GROUP AUDIT & RISK COMMITTEE

The Group Audit & RiskCommittee will at each of the scheduled meetings receive an update report on PHA & PSPS's Strategic Risks and Operational Risks in accordance with the reporting cycle (appendix D). Its role is to:

- Review the Strategic & Operational Risks in accordance with the review cycle (appendix D) at each of its scheduled meetings
- Satisfy itself that all known risks are being actively managed, with the appropriate controls in place and working effectively
- Annually review the group's approach to risk management and approve changes or improvements to key elements of its processes and procedures.

ROLES AND RESPONSIBILITIES – STAFF

ROLE OF THE PHA SENIOR MANAGEMENT TEAM - STRATEGIC

Role

- To ensure that PHA manages risk systematically, economically and effectively through the development of an all-encompassing Risk Management policy.
- To support PHA in the development, implementation and review of the Risk Management policy.
- To share experience on risk, risk management and policy implementation across the group.

Responsibilities

- To have a knowledge of risk management and its benefits.
- Monitor, evaluate and update PHA PSPS 's Strategic Risk Register at least once a quarter
- Review the Risk Management policy, for approval, at least every 5 years.
- As Risk owners each Senior Manager is responsible for:
  - ensuring that appropriate resources and importance are allocated to the process.
  - confirming the existence and effectiveness of the mitigating controls and ensuring that any proposed mitigating actions are implemented.
  - Providing assurance that the risks for which they are Risk Owner are being effectively managed
- Report to each meeting of PHA Audit & Risk Committee on the status of Category A-C risks and the associated controls.
- Ensure risk management and its processes are disseminated and are embedded throughout PHA & PSPS
- Continuous development, promotion & implementation of risk management throughout PHA & PSPS.
- Preparation of relevant business continuity/contingency plans in those areas that are considered high risk.
- To review any training requirements to enable the development & implementation of risk management.

The Chief Executive will take overall responsibility for the administration and implementation of the risk management process across the group.

THE ROLE OF SENIOR MANAGMEMENT TEAM / DEPARTMENT MANAGERS - OPERATIONAL

- To contribute to the management of risk in their own service area / department; and
- To review and update their risks at section meetings in accordance with the reporting cycle (Appendix D).
- To contribute to the development of risk management from a function specific perspective.
- To disseminate the detail of the policy and allocate responsibilities for implementation of the policy in each service area / department.
- To recommend the necessary training on risk management for the employees in the section.
- To share relevant information with other service areas / departments.
- To identify any risk management issues in their service area / department; and
- To ensure that the policy is implemented across their service areas / departments.

ALL STAFF REGARDING RISK MANAGEMENT

All staff have a duty to ensure that risk is managed effectively in their area. This includes engagement with colleagues through formal and informal processes.

All staff have a responsibility for identifying risks in performing their daily duties and taking action to limit the likelihood and impact of these risks.

All staff have a responsibility to provide feedback to Departmental Managers on their experience of implementing risk management and their perceptions of the effectiveness of the approach

7. RISK APPETITE & TOLERANCE

The success of both PHA & PSPS is a result of effectively managing our key risks, which in turn support the achievement of our Strategic Objectives in our Business Plan and associated key targets and priorities. The group acknowledges that an element of risk exists in all activity it undertakes.

Risk appetite is defined as the amount of risk an organisation is prepared to tolerate or be exposed to, should the risk be realised. Too great a risk appetite can jeopardise a project or activity whilst too little could result in lost opportunity.

PHA & PSPS's risk threshold is when the risk is ranked category C or above after controls have been applied (Appendix B). Above this threshold, PHA & PSPS will actively seek to manage the risk and will prioritise time and resources to reducing, avoiding or mitigating these risks.

We have defined above and communicate the organisation's risk appetite and tolerance levels to provide clear guidance on the acceptable level of risk exposure. This helps align risk-taking activities with strategic objectives and ensures that risks are managed within acceptable limits.

The Senior Management Team will agree the appropriate level of risk mitigation activity for each risk is this category. The Audit & Risk Committee will oversee this for risk ranked Category C or higher.

A risk owner will be designated for each risk on the risk register, where appropriate other senior staff may be designated as risk support. Risk owners will ensure that their action plan addresses the risks identified and will be required to monitor the status of their portfolio of risks in accordance with the reporting cycle (appendix D). Risk owners will be reviewed at least on an annual basis.

8. RISK MANAGEMENT PROCESS

The group's risk management process features the following five steps:

Step 1 – Identify Risks

Using PHA & PSPS's (Strategic) or the Department (Operational) objectives, identify the potential threats that could jeopardise their achievement and in turn look at ways to manage these risks.

Risk identification attempts to identify our exposure to uncertainty. Department Heads are ultimately responsible for identifying the risks that their teams may face.

Having identified the risks, these are recorded on the Risk Register template. Where appropriate however, a project level risk register will be maintained for a specific strategic initiative such as a new capital project.

Risks shall be identified at all levels of PHA & PSPS:

- ***Strategic (Board level)***- Where threats and opportunities could affect decisions on PHA & PSPS 's strategic objectives.
- ***Operational (Department Level)*** - Where threats and opportunities could affect decisions on operational actions to meet PHA & PSPS 's strategic objectives.
- ***Project Level*** - Where threats and opportunities could affect the delivery of project targets. (E.g.: entering into major service contracts or partnerships). Before committing to a new business activity, appropriate specialist advice will be sought to supplement our own expertise where appropriate – this may include seeking legal and other professional advice.

Equalities

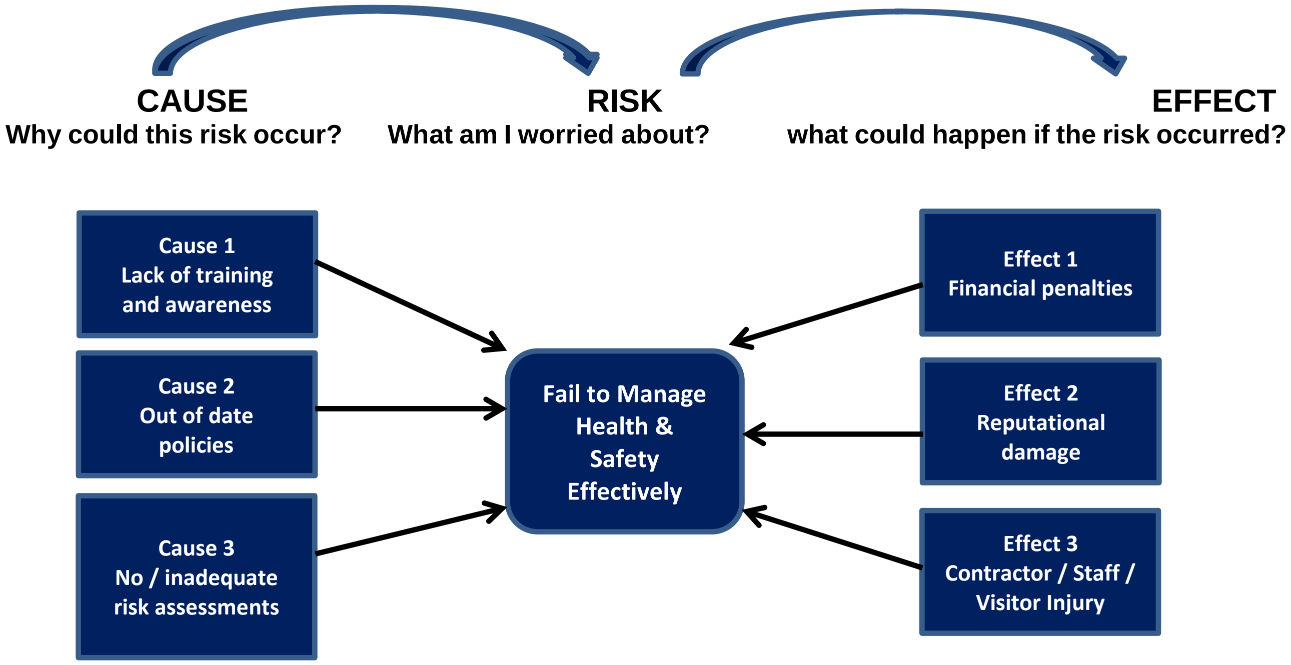
When identifying risk all activities undertaken by PHA & PSPS must be assessed for their compliance with our Equalities and Diversity Policy, and where relevant an Equalities Impact Assessment should be undertaken on the risk or associated risk control processes put in place. We will seek to ensure that there is no risk of discrimination or unfair treatment because of our actions.

Risks, Cause and Effect:

Risks are best expressed using a risk, cause and effect relationship.

Understanding the most important cause helps formulate the best possible actions to manage an uncertainty (i.e. treating the root cause instead of the symptom). Understanding the most important effect helps formulate the best possible contingency plan in case an uncertainty does happen with negative impact.

For example: The Butterfly Effect:


CAUSE
Why could this risk occur?
RISK
What am I worried about?
EFFECT
what could happen if the risk occurred?
Cause 1
Lack of training and awareness
Cause 2
Out of date policies
Cause 3
No / inadequate risk assessments
Fail to Manage Health & Safety Effectively
Effect 1
Financial penalties
Effect 2
Reputational damage
Effect 3
Contractor / Staff / Visitor Injury

From this example we can clearly see what the risk is and also 3 potential causes as to why this risk could occur. We can also see 3 potential effects to PHA & PSPS if this risk was to materialise, therefore if this risk was to be placed on a risk register, we would expect to see 3 controls in place linking to the potential causes of the risk:

Control 1	PHA & PSPS has an extensive and up to date training programme and induction programme that provides all staff with regular training on Health & Safety
Control 2	All Health & Safety policies are held in Central Records and are up to date and all staff have access to this.
Control 3	PHA & PSPS uses a consultant Health & Safety Specialist that undertakes regular audits and inspections to ensure PHA & PSPS are compliant with the up-to-date legislation

Step 2 – Assess Risks

We will regularly identify and assess risks using a systematic and structured approach. This will involve the use of risk registers but may also involve techniques such as risk workshops, risk assessments, and scenario analysis to identify potential threats and opportunities.

Emerging risks will be identified and discussed by PHA Senior Management Team on an on-going basis. Any information that impacts upon PHA or PSPS's risk profile shall be formally assessed, and appropriate action identified and monitored in line with the framework identified in Appendix B

Risks are assessed by looking at the likelihood of the risk occurring and the impact that the risk would have if it were to occur.

Many controls are in place to minimise identified risks. However, in the first instance, risks are assessed as though there are no controls in place i.e. the worst-case scenario or if the controls in place were ineffective. This is known as the '**Inherent'** risk level. The Inherent risk level is recorded in the risk register.

In most scenarios however, there will be controls in place to minimise the impact or likelihood of the identified risk occurring. Risks are therefore assessed based on the Impact and likelihood of the risk occurring considering that there are mitigating controls in place. This is known as the '**Residual'** risk level.

PHA & PSPS's risk register template at Appendix C shows how the Inherent and Residual scores are formatted

Each risk is allocated a risk owner / risk lead whose name is recorded on the risk register. Guidance on how the Impact and likelihood levels of a risk should be assessed can be found in Appendix B

Step 3 – Prioritise Risks

Some risks command a higher priority due to their likelihood and impact.

Both the Inherent and Residual likelihood and impact levels of each risk are plotted and prioritised using a 5 by 5 matrix (***See Appendix B***).

A 'traffic light' system is then used to show Category A to E risks. This results in the prioritisation of both Inherent and Residual risks, which are recorded in the Risk Register.

Red Risks (Category A)

- Risks that fall into the area highlighted as 20 and above will require immediate attention. The status of the risk will require it to be monitored regarding effect on PHA & PSPS's activities and the progress of action taken to ensure its effective reduction.

Amber Risks (Category B)

- Risks that fall into the area highlighted as amber (15-19) may require action and will be actively monitored for any changes in the risk or control environment which may result in the risk attracting a higher score.

Yellow Risks (Category C)

- Risks that fall into the area highlighted as yellow (11-14) will require to be monitored but do not require actions

Green Risks (Category D&E)

- Risks that fall into the area highlighted as green will require annual review only, but no further action

Step 4 – Control Risks

Once the category of a risk has been assessed PHA & PSPS's risk appetite should indicate how the risk is then managed. In managing the risk there will be four categories of response to reduce the likelihood and/or impact of identified risk– transfer, treat, terminate and tolerate. Details of each response can be found in the following table:

Response	Description
Transfer (Risk Sharing)	Risks are transferred to an insurer, e.g., legal liability. However, it must be remembered that this is not possible for all risks. Some service delivery risks can also be transferred to a partner or contractor by way of a formal contract or written agreement. Some aspects of risk however cannot be transferred, for example those that have a reputational impact.
Treat (Risk Reduction)	Risks need additional treatments (controls) to reduce the likelihood and impact levels. This response is most likely where the risk has been identified as a high risk due to the likelihood and impact levels and PHA & PSPS could introduce further controls that will reduce the likelihood and/or the impact of a risk.
Terminate (Risk Avoidance)	A risk maybe outside PHA & PSPS 's risk appetite and PHA & PSPS does not have the ability to introduce additional controls to reduce likelihood and/or impact of the risk therefore there is no other option than to terminate the activity generating the risk.
Tolerate (Risk acceptance)	The controls in place reduce the likelihood and impact levels to an acceptable level (within appetite) and the introduction of additional controls would be cost-benefit prohibitive. It is therefore decided to *tolerate* the risk.

The Senior Management Team will implement effective controls to mitigate identified risks and will regularly monitor the control effectiveness and adjust as needed.

Step 5 – Assurances

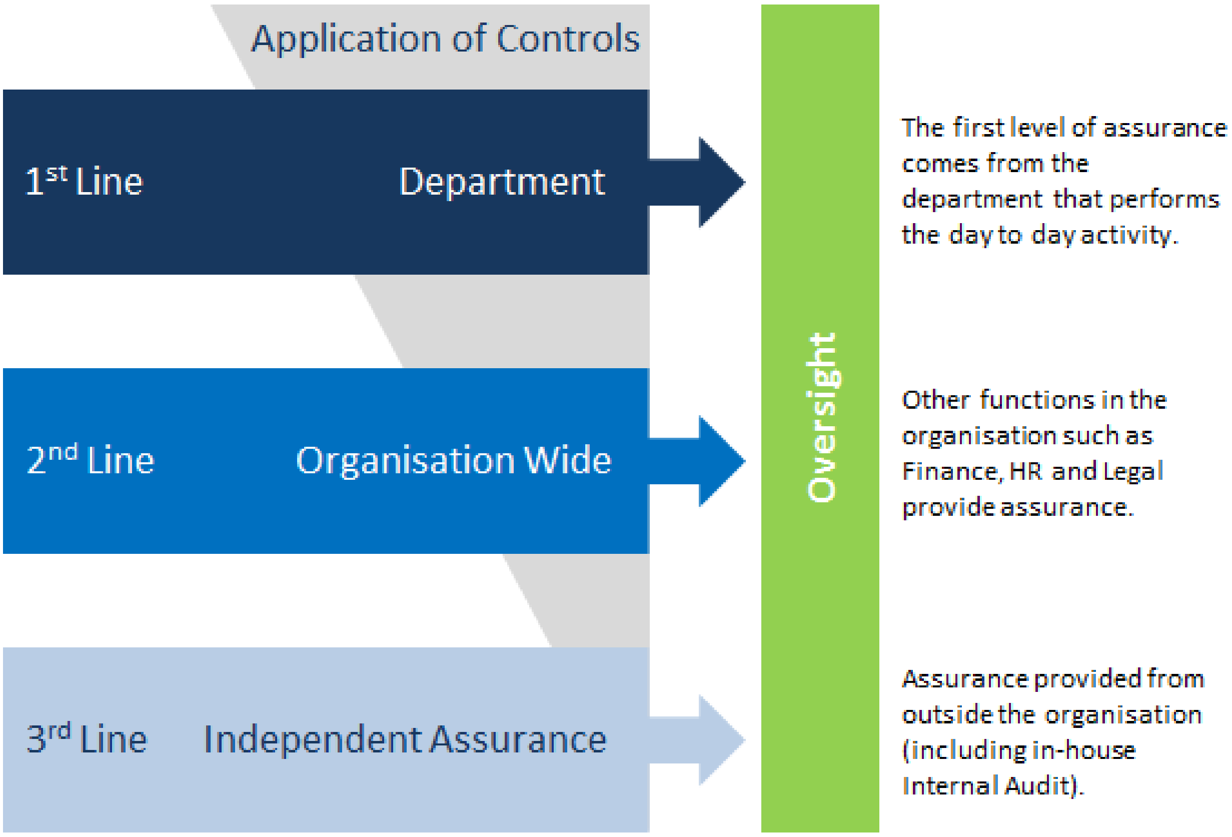
The Senior Management Team will identify and implement appropriate controls to manage the risks identified. PHA & PSPS will also implement processes to give assurance that these controls are working effectively.

What is Assurance?

Assurance:	
Provides:	"Confidence" / "Evidence" / "Certainty"
To:	Department Manager/ Senior Management Team / The Group Audit & Risk Committee / the governing body (individually and collectively)
That:	That what needs to be done (strategically and operationally) is being done

1st, 2nd and 3rd Lines of Assurance

The assurances that PHA & PSPS receives can be broken down into the three-line model as illustrated below and as shown in Appendix C



Application of Controls
1st Line
Department
2nd Line
Organisation Wide
3rd Line
Independent Assurance
Oversight
The first level of assurance comes from the department that performs the day to day activity.
Other functions in the organisation such as Finance, HR and Legal provide assurance.
Assurance provided from outside the organisation (including in-house Internal Audit).

As part of these Assurances PHA/PSPS will implement robust processes for monitoring and reporting on risks to provide timely and accurate information to decision-makers. Using key risk indicators (KRIs) and other metrics to track changes in risk exposure and ensure that risks are effectively managed.

9. RESILIENCE AND BUSINESS CONTINUITY

We will build resilience by developing robust business continuity and crisis management plans to ensure the organisation can respond effectively to disruptions and unexpected events. We will test these plans regularly to identify areas for improvement.

10. INTEGRATION WITH DECISION MAKING

We integrate risk management into strategic planning and decision-making processes to ensure that risks and opportunities are considered when setting objectives and developing strategies. Encouraging risk-based decision making by evaluating the potential risks and rewards of different courses of action.

11. TRAINING & CONTINUOUS IMPROVEMENT

We will continuously review and improve the organisation's risk management practices based on feedback, lessons learned, and changes in the internal and external environment.

We foster a culture of learning and adaptability to respond to evolving risks and challenges. As part of this we will support the provision of training and briefing sessions for relevant staff & Board Members as required. Guidance and support will also be provided by PHA & PSPS through the provision of written procedures/guidance notes and the offer of support from relevant staff.

Through these risk management processes and their continuous improvement PHA/PSPS can enhance its ability to anticipate, assess, and respond to risks effectively, ultimately improving its resilience and long-term success.

12. RISK MANAGEMENT AS PART OF THE SYSTEM OF INTERNAL CONTROL

The system of internal control incorporates risk management. The system encompasses several elements that together facilitate an effective and efficient operation, enabling PHA & PSPS to respond to a variety of operational, financial and commercial risks. These elements include:

Policies and Procedures	Attached to significant risks (e.g. Fire / Health & Safety) are a series of policies that underpin the internal control process. Written procedures support the policies where appropriate
Reporting	The Board of Management, the Group Audit & Risk Committee 7 the Senior Management Team receive key reports on a regular basis which allow for the monitoring of key risks and their control – e.g. monthly spend reports / Quarterly Management Accounts/ Quarterly Risk Report
Business Planning and Budgeting	The business planning and budgeting process is used to set objectives, agree action plans and allocate resources – these take account of risk. Progress towards meeting business plan objectives is monitored regularly
Project Management	All approvals for the execution of new projects include an examination of risk in accordance with the risk appetite of the governing body set out in this policy.
Audit & Risk Committee	The Group Audit & Risk Committee is required to report to the governing body on internal controls and to alert Board members to any serious emerging issues. As part of this function the Group Audit Committee oversees internal audit and external audit. It will review of the effectiveness of the internal control system in its Annual Report to the Board.
Internal Audit Programme	Internal audit is an important element of the internal control process. The annual internal audits should be set based on a risk-based approach.
External Audit	External Audit provides feedback through the Annual Audit Summary Report which will be presented to the Group Audit & Risk Committee on the operation of the internal financial controls it has assessed.
Third Party Reports	On occasions other agencies and consultants will provide reports which will refer to the effectiveness of the internal control systems

13. ANNUAL REVIEW OF EFFECTIVENESS

The Board of Management is ultimately responsibility for ensuring that the Association has in place a system of controls that is appropriate for the business environment in which it operates. These controls are designed to give reasonable assurance with respect to:

- the reliability of financial information used within the Association, or for publication.
- the maintenance of proper accounting records.
- the safeguarding of assets against unauthorised use or disposition

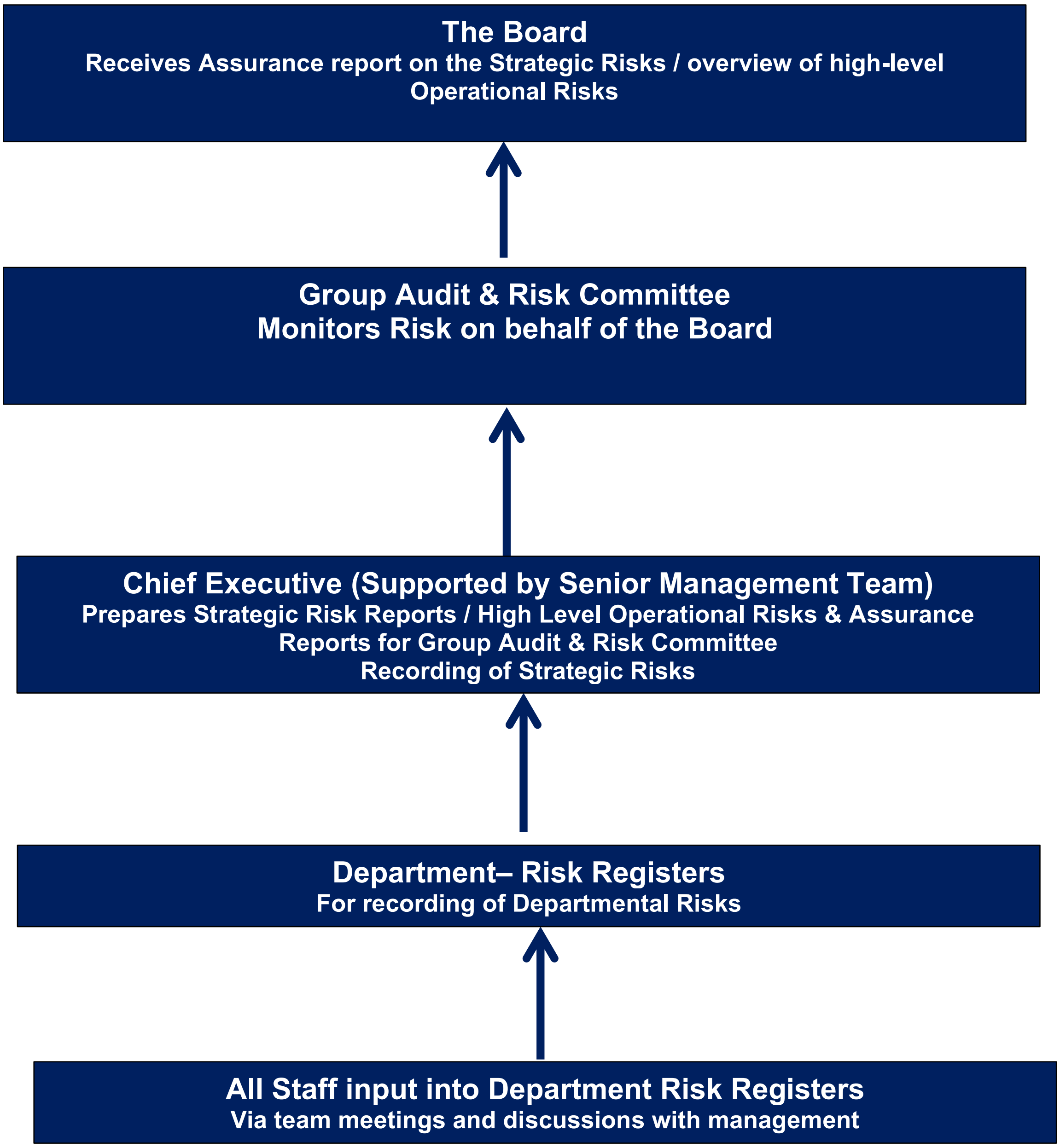
The Board of Management has overall responsibility to establish and maintain systems of Internal financial control and for their effectiveness. Such systems can only provide reasonable and not absolute assurance against material financial misstatement or loss. Key elements of the Association's systems include ensuring that:

- formal policies and procedures are in place, including the ongoing documentation of key systems and rules relating to the delegation of authority, which allow the monitoring of controls and restrict the unauthorised use of Association's assets.
- experienced and suitably qualified staff take responsibility for important business functions and annual appraisal procedures have been established to maintain standards of performance.
- forecasts and budgets are prepared which allow the senior management team and the Board of Management to monitor key business risks, financial objectives and the progress being made towards achieving the financial plans set for the year and for the medium term.
- quarterly financial management reports are prepared promptly, providing relevant, reliable and up to date financial and other information, with significant variances from budget being investigated as appropriate.
- regulatory returns are prepared, authorised and submitted promptly to the relevant regulatory bodies.
- all significant new initiatives, major commitments and investment projects are subject to formal authorisation procedures, through the Board of Management.
- the Board of Management receives reports from management and from the external and internal auditors to provide reasonable assurance that control procedures are in place and are being followed and that a general review of the major risks facing the Association is undertaken.
- formal procedures have been established for instituting appropriate action to correct any weaknesses identified through internal or external audit reports.

The Senior Management Team assist the Board in its review of effectiveness of these systems, though regularly reviewing the effectiveness of PHA & PSPS's risk management & internal control systems and report any required action to the Group Audit & Risk Committee, including on-going identification and evaluation of significant risks and the allocation of resources to address areas of high exposure.

An Audit & Risk Committee Report will be produced annually to provide reasonable assurance on the effectiveness of risk management & internal control systems in place, for consideration initially by the Group Audit & Risk Committee who will then agree a summary report to the Board.

APPENDIX A - Risk Management Reporting and Escalating



The Board
Receives Assurance report on the Strategic Risks / overview of high-level Operational Risks

Group Audit & Risk Committee
Monitors Risk on behalf of the Board

Chief Executive (Supported by Senior Management Team)
Prepares Strategic Risk Reports / High Level Operational Risks & Assurance Reports for Group Audit & Risk Committee
Recording of Strategic Risks

Department– Risk Registers
For recording of Departmental Risks

All Staff input into Department Risk Registers
Via team meetings and discussions with management

APPENDIX B – Risk Matrix and Scoring Criteria –

RISK	Likelihood				
Impact	1	2	3	4	5
	Remote	Unlikely	Possible	Likely	Almost Certain
5 Catastrophic	15	19	22	24	25
4 Significant	10	14	18	21	23
3 Moderate	6	9	13	17	20
2 Minor	3	5	8	12	16
1 Negligible	1	2	4	7	11

Risk Scores	Overall Risk Rating	Review by
20-25	A	Audit Committee
15-19	B	Audit Committee
11-14	C	Audit Committee
7-10	D	Senior Management Team
1-6	E	Senior Management Team

IMPACT

Rating	Rating Scale	Safety	Reputation	Media attitude	Scottish Housing Regulator	Legal Action	Staff	Criminal (including Cyber)	Direct Loss	Regulatory / Industry Status	Service Quality
NEGLIGIBLE	1	No risk of injury. H&S compliant.	External Stakeholders not impacted or aware of problem	No adverse media or trade press reporting.	High compliance standards recognised and rates RSL as Low Risk	Unsupported threat of legal action	Minimal effect on staff.	High control standards maintained and recognised.	Between 0-£10,000	No or little change to regulation in recent history/ near future.	Negligible effect on service quality. Loss of core service for less than 1 day
MINOR	2	Small risk of minor injury. H&S documents not regularly reviewed.	Some external Stakeholders aware of the problem, but impact on is minimal.	Negative general Housing Association article of which PHA or PSPS is mentioned	Regulator rates RSL as Low Risk but verbal comments received	Legal action with limited potential for decision against PHA	Potential for additional workloads intruding into normal non-working time.	Attempted unsuccessful access to operational systems; minor operational information leaked or compromised.	Between £10,001 and £100,000	Limited recent or anticipated changes	Marginally impaired – slight adjustment to service delivery required Loss of a core service for less than 1week
MODERATE	3	High risk of injury, possibly serious. H&S standards insufficient / poor training.	Several Stakeholders are aware and impacted by problems.	Critical article in Press or TV. Public criticism from industry body.	Regulator rates RSL as Medium Risk Findings in written examination report. Potential SHR intervention	Probable settlement out of court	Increase in workloads. Intrusion into normal non-working time.	Logical or physical attack of operational systems.	Between £100,001 and £250, 000	Modest changes recently or anticipated	Service quality impaired – changes in service delivery required to maintain quality Loss of a core service for r than 1week
SIGNIFICANT	4	Serious risk or injury possibly leading to loss of life. H&S investigation resulting in investigation and loss of revenue.	Significant disruption and or Cost to Stakeholders / third parties.	Story in multiple media outlets and/or national TV main news over more than one day.	Regulator rates RSL as High Risk Multiple or repeat governance failings results in SHR intervention	Lawsuit against PHA or PSPS for major breach with limited opportunity for settlement out of court	Significant injuries, potential death. Major intrusion into staff's time.	Police investigation launched; operational data or control systems may be compromised.	Between £250,000 and £500,000	Potential intervention by lead regulator. Significant changes to industry	Significant reduction in service quality experienced Loss of all key services for more than 1week
CATASTROPHIC	5	Multiple fatalities or serious impairment. H&S breech causing serious fine, investigation, legal fees and possible stop notice.	Stakeholders / Third parties suffer major loss or cost.	Governmental or comparable political repercussions. Loss of confidence by public.	Action brought against PHA or PSPS for significant governance failings Forced merger	Action brought against PHA &PSPS for significant breach.	Deaths and/or major effect on staff lives.	Major successful fraud: prosecution brought against PHA & PSPS and Exec for significant failure; Systems totally compromised.	Over £500,000	Major complex changes to industry Intervention on behalf of the Lead regulator	Complete Failure of Services. Loss of all key service for more than 2weeks

LIKELIHOOD				
Rating	Rating Scale	Likelihood	Example of Loss event Frequency	Probability
RARE	1	This will probably never happen / recur	10 years or less frequently	<5% probability
UNLIKELY	2	Do not expect it to happen / recur but it is possible it may do so	Once every 5 years	5-24% probability
POSSIBLE	3	Might happen or recur occasionally	Once every 2 years	25%-49% probability
LIKELY	4	Will probably happen /recur but it is not a persisting issue	Annually	50%-7% probability
ALMOST CERTAIN	5	Will undoubtedly happen /recur, possibly frequently	At least annually	>75%+ probability

APPENDIX C – Risk Register Template

Example Risk Register with Assurances and Action Plan

RISKS Class/Grouping	Risk What am I worried about?	Risk Description 1 - Causes Why could this risk occur?	Risk Description 2- Effect/Impact What could happen if the risk occurred?	Inherent Probability/ Frequency	Inherent Impact / Severity	Inherent Risk Score	1st Line Assurance	2nd Line Assurance	3rd Line Assurance	Assurance Level (Substantial, Adequate , Limited and None)	Residual Probability/ Frequency	Residual Impact / Severity	Residual Risk Score	Tolerate (Risk Acceptance). Treat (Risk Reduction/ Control), Terminate (Risk Avoidance) or Transfer (Risk Sharing)	Further Controls / Actions Required
Budget Control / Procurement	Fail to processes invoices for payment effectively	Lack of staff training or awareness of procedure Procedure out of date Cant access software to process payment Lack of available bank payment authorisers	Debt collection costs Contractors/ suppliers will not work with us Reputational damage	Almost Certain	Catrostophic	25	Purchase Ledger Procedure Separation of duties. Bank Reconciliations Supplier Reconciliations	ICT Disaster Recovery Plan Information security Policy Annual Procurement Report	External Audit Internal Audit - procurement PCIP Assessment Internal Audit of Payment process. TBA	Adequate	Possible	Minor	8	Treat	Complete review of Purchase Ledger Procedure - Aug 24 Review Information Security and Disaster Recover Plan - Sept 24 Complete PCIP assessment by Dec 24,

APPENDIX D – Risk Management Reporting Cycle

The table below sets out the risk management reporting cycle:

Risks	The Board	Audit Committee	Head of Department
Reporting	Annually	Six Monthly	Six Monthly
Policy Review	5 yearly	5 Yearly	Annually
PHA & PSPS 's strategic risks	Annually	Six Monthly	SMT Meetings Monthly
Operational risks which are classified as A	Annually	Six Monthly	SMT Meetings Monthly
Operational risks which are classified as B	Annually	Six Monthly	SMT Meetings Quarterly
Operational risks which are classified as C	Annually	Six Monthly	SMT Meetings Quarterly
Operational risks which are classified as D	N/A	N/A	Departmental On-Going Monitoring
The remaining operational risks that are classified as E	N/A	N/A	Departmental Ongoing Monitoring

APPENDIX E – Glossary of Terms & Risk Categories

Term	Definition
Assurance	An opinion based on evidence gained from the review of PHA & PSPS 's governance, risk management and control framework that risk assessments and control responses are appropriate, adequate and achieving the effects for which it has been designed.
Cause	The reason for the risk exposure – why would a risk occur
Effect	The impact for the risk exposure – what would be the impact if the risk materialised
Exposure	The consequences that arise from the realisation of a risk.
Inherent risk Score	The classification given to a risk, based on its likelihood and potential impact and BEFORE the application of a risk response and controls.
Impact	The effect that a risk would have on us if it occurred.
Likelihood	The probability of a risk occurring.
Risk Owner	The person responsible for ensuring the risk is properly managed and monitored
Residual risk Score	The classification given to a risk AFTER considering the quality of risk responses and controls.
Risk	The threat or possibility that an action or event will adversely or beneficially affect an organisation's ability to achieve its objectives.
Risk appetite	The level of risk PHA & PSPS is prepared to accept or tolerate before considering action necessary.
Risk assessment	The process by which PHA & PSPS identifies and assesses the risks associated with its activities within each level of PHA & PSPS.
Risk management	"Risk Management is the process which aims to help PHA & PSPS understand, evaluate and take action on all our risks with a view to increasing the probability of our success and reducing the likelihood of failure" .
Risk register	A document for capturing important information about each risk PHA & PSPS identifies.
Risk response	An action or process that PHA & PSPS currently has in place to either reduce a risk to an acceptable level or increase the probability of a desirable outcome

Risk Category	Definition
Political	Associated with the failure to deliver either central or local government policies, or recognise their priorities, threats from new policies and legislation.
Financial/ Economic	Associated with financial planning and control. Affecting the ability of PHA & PSPS to meet its financial commitments e.g. internal budgetary pressures, the failure to purchase adequate insurance cover, external macro-level economic changes e.g. market changes.
Social/ Cultural	Relating to the effects of changes in demographic, residential or socio-economic trends on PHA & PSPS's ability to respond and meet its objectives.
Technological	Associated with the capacity to deal with the pace/scale of technological change, or PHA & PSPS's ability to use technology to address changing demands. This may also include the consequences of internal technological failures on the PHA & PSPS's ability to deliver its objectives.
Compliance	Related to possible non-compliance through breaches of legislation e.g. SORP non-compliance, illegality, non-compliance with regulatory requirements, with Health and Safety and/or non-adherence to PHA & PSPS policies and procedures.
Environmental	Relating to the environmental consequences of progressing the organisation's objectives; energy and fuel efficiency issues etc.
Contractual/ Procurement	Under performance against contract specification leading to failure or inability to maintain provision/service; failings in the procurement of services; partners change priorities.
Tenant/ Customer	Associated with failure to meet the current and changing needs and expectations of tenants, clients and customers e.g. service quality, duty of care, or to expose PHA staff or assets to unnecessary risk.
Reputational	A threat or danger to the good name of PHA & PSPS
Strategic	An internal or external event that makes it difficult, if not impossible, to achieve PHA or PSPS Strategic Objectives & Goals
Operational	Lack of control over operations resulting in an inadequate or failing by internal process, people or system; or an external event.

The above risk category table is added for additional information