

FM-POL-03 Risk Management Assurance Policy

Version	6	Developed by	Director of Finance, Governance and Risk
Approval	23/07/2026	In Consultation With	CLT and ARM
Review Period	3 Years	Document Location	Fred- policies and information
Classification Type - (Confidential, Restricted, Internal use only, None)			Internal use only

CONTENTS

1. Policy Purpose
2. Introduction to risk
3. Overview of risk management
4. Roles and Responsibilities in Risk Management
5. Risk Register
6. Risk Appetite
7. Inherent Risk
8. Risk reporting
9. Categorising Risk
10. Assessing Risk
11. Implementation and Monitoring of the Policy

1. Policy purpose

1.1 The purpose of this policy is to:

- i. Define Frameworks risk management approach.
- ii. Set out the risk management systems to support delivery of the Strategic Plan and to continuously improve services, both in quality and delivery, by managing the risks involved.
- iii. Enable framework to take up new opportunities and undertake new business knowing that any associated risks have been identified, are acceptable and are being managed
- iv. Protect the assets.
- v. Ensure risk management is embedded as a routine activity and forms part of Framework's culture, decision making processes and internal control framework.

2. Introduction to Risk

- 2.1 Risk is the effect of uncertainty on the achievement of Framework's Strategic Priorities. Risks may arise from internal or external factors and may affect the delivery of strategic, operational, financial, regulatory or service priorities. This Policy is primarily concerned with the management of negative events, i.e., risks rather than opportunities.
- 2.2 Almost all of Framework's activities entail a degree of risk.
- 2.3 Risk management is the process by which risks are identified, evaluated, controlled, and monitored. Framework's aim is to identify, manage and minimise risks which may prevent the organisation achieving its priorities. This is achieved through the processes of risk management. Framework seeks to ensure that risk management processes are embedded throughout all levels of the organisation, via its governance structures, its systems and controls and the behaviours of all employees including volunteers and the Board. The management of risk is a continuous process, involving regular monitoring and adjustment as necessary.
- 2.4 Framework promotes a positive risk culture where employees, volunteers, managers and Board members are encouraged to identify, discuss and escalate risks openly. Risk management supports informed decision-making, organisational learning and continuous improvement.

3. Overview of Risk Management

- 3.1 Framework's approach to risk management is to identify risks; assess and score risks in terms of likelihood and impact; assign ownership; identify and implement controls; and take action, where possible, to reduce the likelihood and/or impact of risks materialising.
- 3.2 Risks are identified through a variety of sources including operational activity, strategic planning, incident reporting, audit activity, horizon scanning, environmental analysis, governance reporting and day to day risk assessment activity undertaken by employees. Risks related to the achievement of the strategic priorities are recorded on Framework's risk register and reviewed monthly by the Senior Leadership Team (SLT) to ensure that the risk register remains up to date.
- 3.3 The risk register identifies, assesses, and records the actions being taken in respect of strategic risks. These risks are presented on the heat map. The heat map is a graphical representation of the risks in the register and their risk scores. The heat map is presented to show the raw risk scores before the application of controls and the residual risk scores after controls.
- 3.4 The Board, Committees, management and employees at Framework have clearly defined responsibilities for identifying, managing, monitoring and responding to the risks recorded within the risk register.
- 3.5 The risk management and internal control systems are embedded in Framework's day to day operations and are designed to be capable of responding quickly to evolving business risks, whether they arise from internal or external factors.
- 3.6 Often it is not possible to eliminate risk, without halting the related activity. Therefore, the aim of risk management is the minimisation of risk, rather than its elimination.
- 3.7 A diagram of the Risk Management Methodology is provided at **Appendix A**.

4 Roles and Responsibilities in Risk Management

The Board

- 4.1 The Board is ultimately responsible for ensuring that Framework achieves its purpose and priorities. Risk management and mitigation is part of the context in which decisions are made by the Board. The Board Report Template has a specific impact assessment of risk.
- 4.2 Board determines Framework's risk appetite and acceptable levels of risk tolerance. The Board also oversees the progression of strategic activities associated with reducing risk levels.
- 4.3 The Board is responsible for ensuring the design and implementation of appropriate risk management and internal control systems that identify the risks faced by the organisation and appropriate methods of mitigation.

- 4.4 The Board is responsible for monitoring and reviewing effective systems of risk management and a framework of internal controls throughout the organisation and satisfying itself that they are functioning effectively.
- 4.5 Board reviews and approves this Risk Management Policy at least every three years on recommendation of the Audit and Risk Management Committee.
- 4.6 The Board approves The Statement of Internal Controls Assurance annually on the recommendation of the Audit and Risk Management Committee.
- 4.7 The Board ensures that Framework's financial plans are sufficiently robust to manage potential scenarios that could happen. A risk analysis accompanies the approval of the annual budget. The Long-Term Financial Plan is stress tested aligned to the risk register with mitigating actions identified and quantified within the Financial Resilience Statement.

The Audit and Risk Management Committee (ARM)

- 4.8 In accordance with its terms of reference the ARM will monitor the Risk Register and accompanying information. Ensuring appropriate management action is taken.
- 4.9 On behalf of the Board the Audit and Risk Management Committee has specific responsibility to scrutinise, to monitor and have oversight of the expectation of any change to get to the required level and associated timelines in particular for high rated risks. The ARM may require an in-depth review on any particular risk to be reported back to the Board as part of its assurance work. As part of its assurance responsibilities, the ARM undertakes detailed reviews of individual strategic risks, including consideration of the effectiveness of controls, sources of assurance and any assurance gaps.
- 4.10 The ARM can commission external independent support as required to fulfil its terms of reference, it may seek guidance from the Company Secretary as support.
- 4.11 The ARM Committee receives assurance regarding business continuity and organisational resilience arrangements to support Framework's ability to respond to significant adverse events.
- 4.12 The ARM will specifically consider and make recommendation for approval on the following items:

- i. The Statement of Internal Controls Assurance
- ii. Risk Management Policy

The Senior Leadership Team (SLT)

- 4.13 The Chief Executive and Directors form the Senior Leadership Team (SLT).
- 4.14 The SLT meets fortnightly and reviews the risk register and heat maps monthly.

- 4.15 Risks are assigned to members of the Senior Leadership Team who have responsibility for managing, monitoring, controlling, and reporting risk.
- 4.16 The Chief Executive updates the Board at every meeting on significant activities, including related risks, via the Chief Executive's report.
- 4.17 The Director of Finance, Governance and Risk is the SLT lead for risk management and the maintenance and development of Framework's risk management framework.

The Corporate Leadership Group (CLG)

- 4.18 The SLT and Assistant Directors, together form the Corporate Leadership Team (CLT).
- 4.19 Matters arising from CLT meetings inform the monthly SLT risk review process and support the identification of new and emerging risks.
- 4.20 The risk register and risk maps are circulated to CLT members quarterly.
- 4.21 CLT are responsible for managing and monitoring operational risks within service areas. Levels can be escalated from operational to strategic risks.

Internal Audit

- 4.22 Internal Audit plays a key role in evaluating the effectiveness of policies and procedures and the management of associated risk. The ARM approves an annual programme of internal audits, which is devised with reference to the risk register and then monitors the progress of this including the implementation of recommendations.
- 4.23 Internal Audit provides independent assurance to the Board and ARM regarding the effectiveness of governance, risk management and control arrangements.

All Employees and Volunteers

- 4.24 This risk management policy sets out defined processes for managing risk, but successful risk management can only be accomplished on a day-to-day basis by Framework's employees and volunteers. This is achieved through the design and communication of relevant policies and procedures relating to all areas of activity and operation which are followed by them in their work.
- 4.25 Employees and volunteers are expected to identify, report and escalate risks appropriately as part of their day to day responsibilities.

5 Risk Register

- 5.1 The risk register collates Framework's principal strategic risks into a single document. The impact of each risk is defined and recorded in the context of achieving the Strategic Plan priorities.

- 5.2 The controls and mitigations in place, together with planned actions and expected improvements, are recorded within the risk register. Mitigations are considered in the context of the three lines of defence model. Additional supporting information may be included where required. Each risk is aligned to relevant Strategic Plan priorities and, where appropriate, associated Key Performance Indicators. An example of the Risk Register is provided at **Appendix B**.
- 5.3 Framework recognises the importance of quality data in supporting effective risk management, assurance and informed decision making.
- 5.4 The risk register forms part of Framework's wider assurance framework and is used to inform internal audit planning, Board assurance, stress testing, resilience planning and performance monitoring.
- 5.5 Significant changes to risk scores, controls, mitigating actions, assurance arrangements or risk exposure will be recorded through the risk register review process and reported through the governance framework.
- 6. Risk Appetite**
- 6.1 The Board and Senior Leadership Team have developed a risk appetite statement which records the way Framework views the different areas of risk facing the organisation.
- 6.2 The statement supports strategic decision making by identifying areas of operation and activity where Framework may be prepared to accept greater levels of risk in pursuit of its Purpose and Priorities.
- 6.3 A risk appetite score is assigned to each area within the risk appetite statement. Risks assessed above appetite are subject to ongoing review and mitigation activity, with actions identified to reduce exposure where possible. Where a risk remains above appetite, the Board will maintain oversight of the risk, the actions being taken and the rationale for any continued acceptance of the level of inherent risk. The risk appetite is represented by a black line on the heat map to demonstrate Framework's tolerance for risk within each area.
- 6.4 The current Board-approved risk appetite statement is shown at **Appendix C**. This records Framework's willingness to take risks in particular areas to achieve our stated objectives. The willingness to take risks is classified in terms of hunger.
- 6.5 The risk appetite is reviewed and approved by the Board annually. References to risk appetite appear within Board and Committee papers to support informed discussion, challenge and decision-making. Risk appetite provides the context in which the risk register is reviewed and understood.

7 Inherent Risks

- 7.1 Framework recognises that some risks are inherent to the specialist nature of its services, the people it supports and the environment in which it operates. In some cases, despite effective controls and sustained mitigation activity, the residual risk score may remain above the approved risk appetite. Where a risk remains above appetite, the disparity remains visible within risk reporting to ensure continued oversight by the Board and Senior Leadership Team.
- 7.2 The identification of an inherent risk does not reduce the requirement for ongoing management, monitoring, assurance or mitigation activity. Framework will continue to seek proportionate opportunities to reduce risk exposure where these are achievable and consistent with available resources.
- 7.3 Inherent risks are identified within the risk appetite statement and remain subject to routine review through the risk register, heat maps, Audit and Risk Management Committee and Board reporting arrangements.

8 Risk Reporting

- 8.1 The risk register and heat maps are considered monthly by the Senior Leadership Team. The Senior Leadership Team has responsibility for the ongoing identification, management, monitoring and escalation of risks.
- 8.2 The Audit and Risk Management Committee considers risk at each meeting. The Committee also reviews relevant sector intelligence, regulatory guidance, horizon scanning information and emerging risks affecting Framework's operating environment. This information is used to support continual improvement, organisational learning and effective risk management.
- 8.3 The Board considers risk as part of each Board Meeting agenda, this will include any items referred from the Audit and Risk Management Committee. There is a requirement for the Committee to raise any matters of concern or issues relating to their remit to monitor the Risk Register and have oversight that the appropriate actions are taken, including the expectation of any change to get to the required level and associated timelines in particular for high rated risks and any significant assurance concerns or gaps identified through governance, compliance or audit activity.
- 8.4 Each Board Meeting and Committee has a standing item of risk at the end of each agenda to establish if the business concluded creates a new risk or any changes to the existing risks on the risk register.
- 8.5 Framework will identify emerging risks through horizon scanning, environmental analysis, strategic planning activity, operational intelligence, governance discussions and external sector information. Significant emerging risks will be considered through the Audit and Risk Management Committee and escalated to the Board where appropriate.
- 8.6 The ARM Committee undertakes, detailed reviews of individual strategic risks to provide assurance regarding the effectiveness of controls, sources of



assurance, planned mitigations and any assurance gaps requiring further consideration.

9 Categorising Risk

9.1 Framework's risk register, groups related risks together aligned to the risk appetite statement using the following categories:

- i. Legal, Regulatory and Compliance
- ii. Infrastructure and Internal Service
- iii. Human Resources
- iv. Financial and Treasury Management
- v. Asset Management and Property Development
- vi. New business, Contracts and Revenue development
- vii. Fundraising and Public Relations
- viii. Governance

9.2 Each risk is assigned to one of the above categories. The Board delegates responsibility for each individual risk to the appropriate risk owner who is member of the Senior Leadership Team with delegated responsibility for taking action to manage or mitigate the identified risk. The Board reserves the right to retain the ownership of a particular risks as appropriate.

10 Assessing Risk

10.1 Risks are assessed according to their likelihood and impact. Framework uses a clear structure of a five-scale rating for both likelihood and impact. The ratings are as follows:

The timeframe on likelihood refers to the change of a single or multiple occurrences over a five-year period.

Likelihood	Guidance	Probability	Frequency
Rating 1 Rare	Could occur at some time, but unlikely to happen within the next 12 months.	Once every 5 years	0.2
Rating 2 Unlikely	May happen at some time, may occur once every 3 years.	Once every 3 years	0.35
Rating 3 Possible	Might happen at some time, may occur once every 2 years.	Once every 2 years	0.60
Rating 4 Likely	Will probably happen over the next 12 months	Once per year	0.70
Rating 5 Almost Certain	Will happen over next 12 months	Quarterly	0.90

Impact assessment

Rating and generic impact description	Examples of the impact of each rating			
	Financial	Health and Safety	Service Delivery	Organisational Reputation
Rating 1 Insignificant	<£50k	Breach limited to one area with no onward regulator reporting required. Contained within existing budget resources	Short term (<14 days) disruption across narrow scope (e.g., up to two site operations)	Minor stakeholder interest. Expected to have little material impact on support
Rating 2 Minor	£50k-£250k	Scrutiny required by external agencies (i.e., HSE/Fire etc. RIDDOR reportable event) may include formal enforcement action.	Longer term disruption (>28 days – 56 days) across narrow scope. Temporary disruption (14 – 28 days) across limited scope (e.g., up to four operations)	Dome negative influence on stakeholders putting at risk support to Framework services limited to one pillar.
Rating 3 Modest	£250k - £1M	Major breach resulting in major injury. More than one RIDDOR and external regulator reporting.	Longer term disruption (>56 – 90 days) across limited scope. Temporary disruption across a wide scope (e.g., up to 5 operations)	Negative influence on significant stakeholders putting at risk support to Framework services/funding limited to two pillars
Rating 4 Major	£1M-£1.5M	Significant breach resulting in single death or major multiple injuries. Several RIDDOR and external regulator involvement	Longer term disruption across broader scope. Temporary disruption across a wide scope (e.g., up to 6 operations)	Negative influence on significant stakeholders putting at risk support to Framework services/funding limited to three pillars
Rating 5 Catastrophic	>£1.5M	Significant breach(es) evoking regulator intervention Multiple deaths	Temporary or longer-term disruption across broadest scope. (e.g., from 6 - all 9 operations)	Negative influence on significant stakeholders putting at risk support to Framework services/funding across Framework

- 10.2 The individual scores are multiplied together to give an overall risk score. On the risk register, the risk score is calculated before and after the effects of relevant controls. The action of controls brings the risk score down to leave a residual risk calculation:

$$\text{Likelihood} \times \text{Impact} = \text{Score (L} \times \text{I} = \text{S)}$$

- 10.3 This method of assessing and scoring risks produces 25 possible resulting risk values ranging from 1-25. The risks are rated as High, Medium, and Low based on the following scoring and is presented below utilising a grid format.

Very High Risks - score of 20 or more

High Rated Risks – score of 15 to 19

Medium Rated Risks – score of 10 to 14

Low Rated Risks – score of 5 to 9

Minimal 0 – 4

Probability	5	5	10	15	20	25
	4	4	8	12	16	20
	3	3	6	9	12	15
	2	2	4	6	8	10
	1	1	2	3	4	5
		1	2	3	4	5
		Impact				

- 10.4 Framework displays the results on a heat map which shows total risk score for each risk and is colour shaded (red, amber, green) with the thresholds for the rating marked. This very quickly identifies the risks with the highest total score.
- 10.5 The “before controls” map shows the raw scores before controls. The “residual” map shows the scores after the application of relevant controls.
- 10.6 An example of the heat map is provided at **Appendix D**.

11 Implementation and Monitoring of the Policy

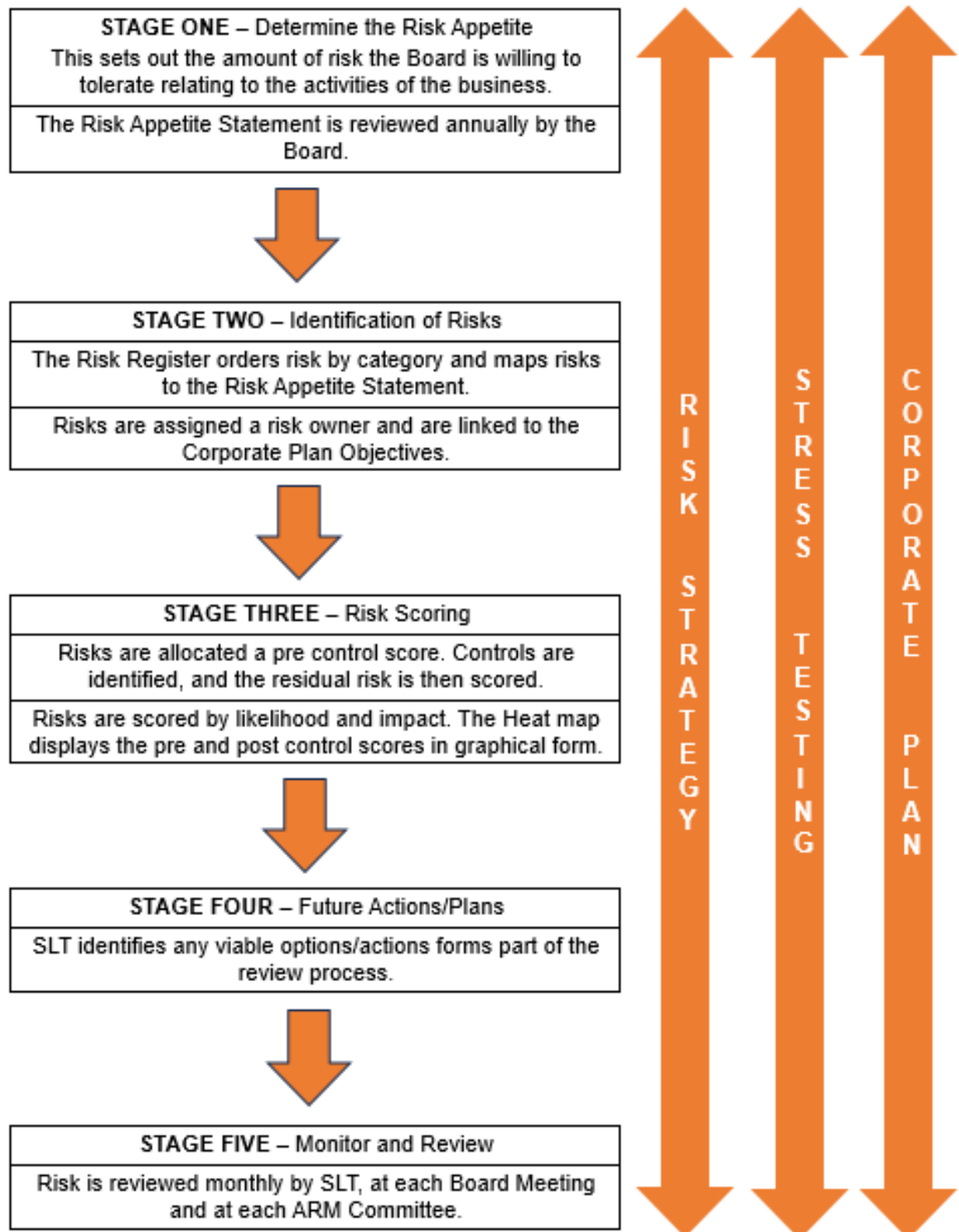
- 11.1 The implementation and monitoring of this Policy, and the reporting of this to the Board, will be actioned through the following activities:
- Annual review and updating of the risk appetite statement.
 - Presentation of the Risk Register and Heat Map at each Board Meeting.
 - Specific consideration of risk at each meeting of the Audit and Risk Management Committee, with provision for onward reporting to the Board if necessary.



- iv. Consideration of emerging risks, horizon scanning and relevant sector intelligence through the Audit and Risk Management Committee and Board reporting processes.
- v. Implementing the three lines of defence model within the controls detailed on the risk register.
- vi. Deep dives into strategic risks to provide assurance regarding the effectiveness of controls, risk management arrangements and sources of assurance.
- vii. Annual review of the Financial Resilience Statement as part of the Stress Testing of the Long-Term Financial Plan.

This Policy will be reviewed on a three yearly cycle – the next review is due in December 2029.

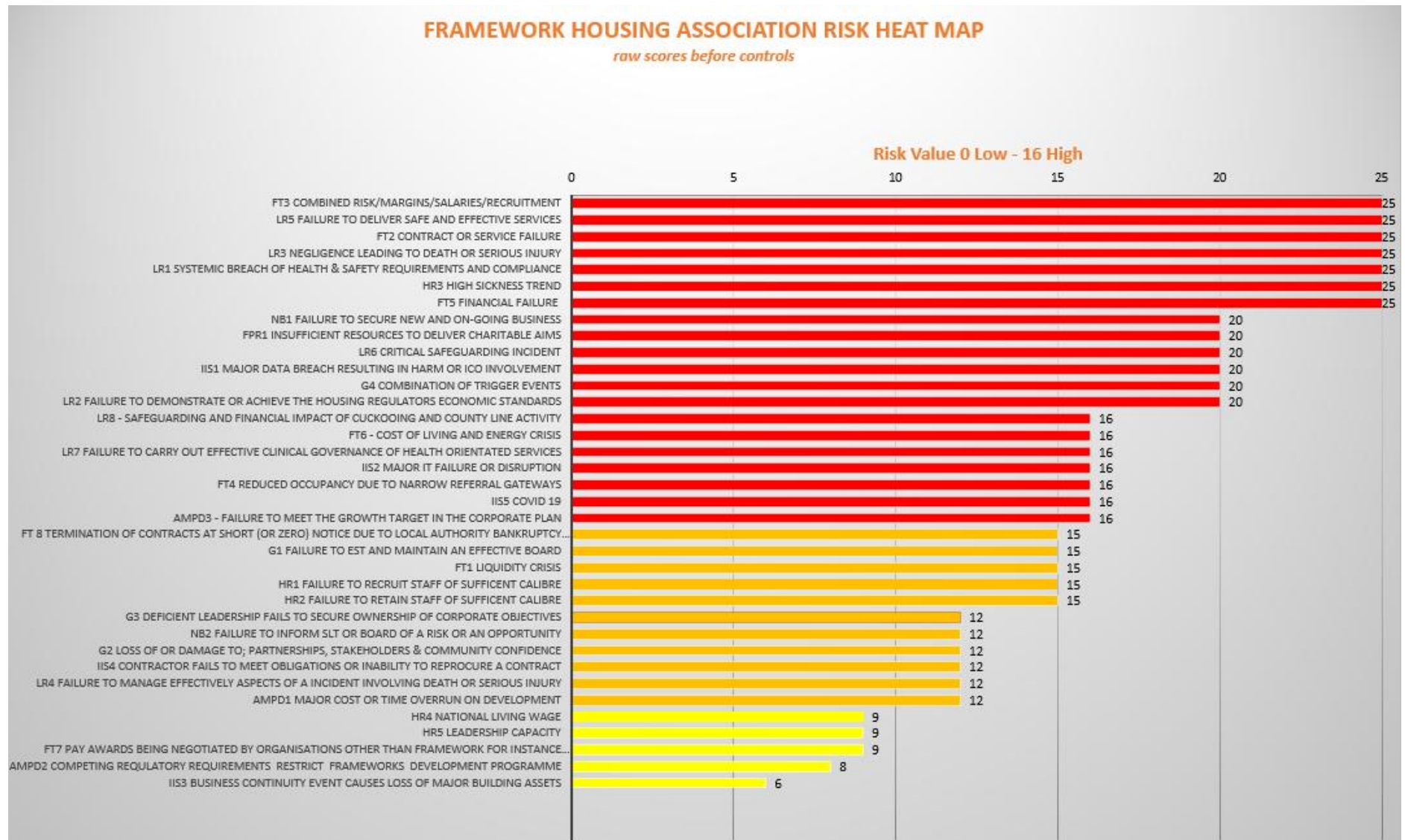
Appendix A – Risk Management Methodology



Appendix B – Example of the Risk Register

Count	Organisation Area	Risk Ref.	Risk Name	Impact	Likelihood	Impact	Value (L x I)	Controls	Owner	Net Likelihood	Net Impact	Net Value	Risk Appetite target	Appetite Reference	Notes or changes from last review	Corporate Plan Link by Objective
1	Regulatory Compliance	LR1	Significant breach of Health & Safety requirements and compliance	Framework: fines, reputational damage, possible loss of contracts. Individual: possible harm.	5	5	25	Suite of H&S policies in place and regularly reviewed. Staff induction and training programmes. In house Health and Safety Manager, Fire Safety Officer and Compliance Team . Incident reporting, KPI dashboard and Board KPIs. Employment of specialist contractors (e.g. water testing, electrical testing, gas servicing). Datix and C365 systems. H & S Action plan and associated reporting to the Board. Internal Quality Team deployment. Peer Audit processes.	DN	2	4	8	2	4	Related Risks OD 1,2,6,7. Related KPIs - Gas Servicing %, Serious and Untoward Incidents . Health and Safety reporting.	2
2		LR2	Failure to demonstrate or achieve the Housing Regulator Economic Standards	Budget overspend, LTFF not delivered, Regulatory intervention, Reputational impact, Reduced Funding opportunities	4	5	20	Monthly management accounts and quarterly detailed reporting to the Board. VFM Strategy and Plan in place. Board annual self assessment. VFM metrics and local metrics reported in annual accounts, Regulator rating G1 - V2. Annual LTFF and stress testing (or as required). Targets in Corporate Plan and associated actions. Operational focus, voids, bad debts, energy, service transformation, commissioner negotiations.	SW	3	3	9	4	3	Our assumptions come from a specialist provider, this is changing rapidly and so to take account we will exceptionally update the LTFF and assess impact of inflation and interest rates on the LTFF.	2
3		LR3	Negligence leading to death or serious injury	Loss of reputation, legal liability, loss of contracts, harm to individuals. Future risk adversity.	5	5	25	Policy Framework, Incident management processes, HR and supervision processes including training, induction and management. Board scrutiny of KPIs and H&S performance.	AR	1	4	4	2	4	Related KPIs Serious and untoward incidents, Contractual Targets, urgent repairs, emergency repairs, Gas servicing, Health and Safety, Whistle Blowing.	2
4		LR4	Failure to manage effectively aspects of a incident involving death or serious injury	Loss of reputation, negative PR, loss of contracts, resources realigned to mitigate	4	3	12	Dedicated communication resource. Developed relationships with media, SUL learning and continual improvement, business continuity testing	AR	3	2	6	8	4/5		2

Appendix C – Example of the Heat Map





Appendix D – Example of the Risk Appetite Statement



Organisation Area	Detail	Reference	Proposed Score	Very High	High	Medium	Low	Minimal
Scoring				21 - 25	16 - 20	11 - 15	06 - 10	01 - 05
Legal & Regulatory Compliance	Internal & External Audit	1	11					
	Regulatory compliance: Care Quality Commission	2	7					
	Regulatory compliance: Regulator of Social Housing	3	4					
	Significant breach of Health & Safety requirements and/or compliance *	4	2					
	Regulatory compliance – Others	5	9					
	Safeguarding – incidents *	6	3					
	Failure to manage aspects of an incident involving death or serious injury.	7	8					
Human Resources	Recruitment – Process	8	12					
	Recruitment – Approaches	9	18					
	Failure to recruit and retain sufficient staff of the requisite quality *	10						
	Staff Satisfaction – Outcome	11	11					
	Staff Satisfaction – Strategies	12	17					
	Use of volunteers	13	21					
	Promotion and delivery of the Equality, Diversity, and Inclusion Action Plan	14	12					
	Employment of former service users	15	18					