

IronOak



IRON OAK

RISK MANAGEMENT FRAMEWORK

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

Control Sheet

Version number	02
Date approved by Board	30 March 2026
Date of next review	February 2027
Status	Published
Policy owner	Company Secretary
Policy location	IronOak Shared Drive/BrightHR
Target group	Employees

Document History:			
Version	Date of review	Author	Note of revisions
01	March 2025	Head of Governance	New Policy

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

1. Introduction

- 1.1. The purpose of the Risk Management Framework (the Framework) is to set out IronOak Homes (IronOak) approach to identifying, evaluating and managing the risks it faces as a Registered Provider and comprises of IronOak's Risk Management Policy and Risk Management Procedure.
- 1.2. Successful implementation of the Framework and the management of risks will support IronOak's long-term viability, deliver compliance with the National Housing Federation's (NHF) Code of Governance 2020 and ensure adequate levels of risk control measures are in place. It also supports a 'Risk Managed Culture' whereby all IronOak staff (regardless of level) have an appropriate regard and consideration of operational and strategic risks with a key objective, whenever possible, to reduce those risks to within a level of acceptability as defined by the members of the Board.
- 1.3. A Glossary of Risk Terms has been created (Appendix 1) to ensure a consistent understanding of the terms used with this Framework.
- 1.4. The Chief Executive Officer and the Company Secretary (or related role) are responsible for ensuring the Risk Management Framework is adhered to.

2. Purpose

- 2.1. Risk Management is a mechanism which seeks to identify, evaluate and manage risks to the achievement of IronOak's objectives, as well as allow for effectiveness of our controls to assist in taking new opportunities.
- 2.2. IronOak is committed to embedding a framework and culture within the organisation to enable the identification of risks which may adversely affect its assets, interests or business objectives and those of its stakeholders. It is a key objective of the organisation wherever possible to reduce those risks to within a level of acceptability defined by members of the Board. In doing so, it is also the policy of the organisation to minimise and contain the costs and consequences incurred in the event of harmful or damaging incidents arising from those risks and to provide for adequate and timely compensation, restoration and recovery.
- 2.3. The Risk Management Policy outlines the requirements, as set by the Board, of all staff in successfully delivering and embedding an effective Risk Management Framework within IronOak.
- 2.4. The Chief Executive Officer and the Company Secretary (or related role) are responsible for ensuring the policy is adhered to.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

3. What is Risk Management – Definition

- 3.1. ISO 31000 Risk Management defines risk as ‘the **chance** of something happening that will have an **impact** on **objectives**. The impact may be positive or negative and thus a risk can be an opportunity or a threat.
- 3.2. Risk management is the structured formal approach to managing uncertainty related to a threat or opportunity, including the activities to manage the risks and the tactics, structures and controls employed to mitigate any potential exposures.
- 3.3. The objectives of risk management are to:
- Promote transparency by ensuring that key business risks are identified, articulated and communicated to the right people in a timely manner.
 - Ensure that appropriate relevant and practicable controls are employed to mitigate exposure and/or optimise competitive advantage.
 - Ensure that the company’s risk appetite, as articulated by the Board and Audit & Risk Committee (ARC) is uniformly applied.
 - Encourage informed decision-making through analysis of risk.
- 3.4. The organisation’s approach to risk provides increased assurance to stakeholders on the standard of governance applied and, as the total risk and control environment is visible, it contributes to the strategic and tactical decision-making processes.

4. Legal and regulatory requirements

- 4.1. As a Registered Provider, IronOak must adhere to the Regulator of Social Housing’s (RSH) Regulatory Framework for social housing in England. The Governance and Financial Viability Standard sets out the following requirements in relation to risk:
- RPs must have an effective risk management and internal controls assurance framework in place. RPs shall ensure that they have an appropriate, robust and prudent business planning, risk and control framework.
 - RPs shall manage their resources effectively to ensure their viability is maintained while ensuring that social housing assets are not put at undue risk. The framework shall ensure the financial and other implications of risks to the delivery of plans are considered. RPs shall carry out detailed and robust stress testing against identified risks and combinations of risks across a range of scenarios and putting appropriate mitigation strategies.
 - IronOak has adopted the NHF’s Code of Governance 2020 that requires members to actively manage their risks, and obtain robust assurance that controls are effective, plans and compliance obligations are being delivered, and that the organisation is financially viable.

5. Benefits of effective risk management

- 5.1. Effective management of both strategic and operational risks in an uncertain operating environment has the potential to bring a number of benefits:

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- Improved strategy, with informed strategic objectives being set.
- Enhancement of reputation through anticipating and responding better to threats and opportunities.
- Improved management of operations, including customer focus and service delivery.
- Proactive approach to addressing legislative/regulatory requirements.
- Ability to allocate resources to where they would deliver the greatest impact.
- Improved control and management of finances, allowing better decision making.

6. Risk roles & responsibilities

Whilst Risk Management is the responsibility of every member of staff, the below outlines the main responsibilities attached to each of the following roles / groups:

6.1. The Board

Under the NHF's Code of Governance, the Board retains ultimate strategic responsibility for risk management and ensuring that appropriate risk management arrangements are in place. In line with the organisations Rules, the IronOak Board has delegated the detailed scrutiny and evaluation of risk to the Audit and Risk Committee (ARC) with regular reporting back to the Board. (see section 5.2).

The Board's specific responsibilities in relation to risk are:

- Ensuring a suitable risk management framework is in place to ensure it understands IronOak's risk profile and the effectiveness of key controls.
- Establishing and documenting its appetite for the risks the organisation faces in pursuit of its strategy
- Ensuring that IronOak is resilient to the risks it may face, with appropriate mitigations and a suitably comprehensive, tested and up-to-date business continuity plan.
- Members have the skills and experience appropriate to the level and type of risks faced.
- Review the Strategic Risk Register at least twice a year. This includes the risks associated with activities carried out by subsidiaries or partnership vehicles
- Regularly participating in stress testing its plans to identify the risks (or combination of risks) that may pose a material threat to the viability of the business and ensure that appropriate mitigations are in place.
- Ensures the annual report includes a statement about its risk management work, including its understanding of strategic and emerging risks and how these are being managed or mitigated.
- Manages the organisation in a crisis.

The Terms of Reference for the Board are reviewed annually and sooner, if required by regulatory and/or legislative changes.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

6.2. The Audit & Risk Committee

With delegated responsibility from the Board to oversee compliance with the statutory duties, provide assurance on the systems of internal control, risk management and the internal and external audit functions to ensure that they are effective and well-managed, the ARC will:

- Formulate strategy and policy based on risk appetite, risk attitudes and risk exposures.
- Oversee the Risk Management structure and processes.
- Pro-actively challenge the Executive Leadership Team and Senior Management on risk matters, monitoring delivery of actions and their effectiveness in mitigating risk.
- Undertake horizon scanning on sector and global risks.
- The Terms of Reference for ARC are reviewed annually and sooner if required by regulatory and/or legislative changes. The Committee's core responsibilities in relation to risk management are:
 - Review and recommend to the Board for approval the risk management appetite, strategy and policy.
 - Review and monitor the adequacy and effectiveness of the risk management systems with frequent updates to the Board.
 - Ensure that the Executive Leadership Team embeds risk management throughout the organisation.
 - Review the key strategic risks quarterly and recommend them to the Board for approval.
 - Scan and advise the Board on emerging and future risks that potentially impact on the organisation.

ARC, as the delegated committee for risk management, will meet at least annually with the Executive Leadership Team to:

- Review this Framework to ensure it remains fit for purpose.
- Review the Risk Matrix and definitions for measuring the impact and likelihood of risks occurring (see section 3.10).
- Receive/discuss the RSH's annual report on the Sector Risk Profile to identify any possible impact on IronOak's activities
- Discuss stress testing arrangements in place and the scenarios being used to provide assurance they are acceptable and sufficient to meet the requirements of the Governance and Financial Viability Standard (See Section 4).
- Set the Board's appetite for risk (see Paragraph 2.13 and section 4).

6.3. Chief Executive Officer

Responsibility for maintaining a sound system of internal control that manages the key operational and strategic risks, reporting on risks and uncertainties and principal risks within the Annual Report to the Board.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

6.4. Executive Leadership Team & Operational Management Team

Contributes towards the identification and management of operational, strategic and cross-cutting risks, making recommendations to ARC for any emerging risks to be added to the Strategic Risk Register to include:

- Building a risk aware culture within own departments, setting a positive tone to support Risk Management.
- Understanding the Board's risk appetite and managing strategic, business and project objectives within the appetite levels established.
- Ensuring key strategic and business risks are adequately owned, assessed and mitigated. Reviewing sector risks, organisational risks and related assurance mechanisms.
- Implementing planned mitigation to manage owned risks by ensuring delivery of appropriate action plans which have sufficient resources attached and are aligned to the wider business activity / priorities.
- Reviewing and reporting on progress with planned mitigating actions.
- Identifying and reporting on changed circumstances / risks to the Governance and Assurance Manager (or related role), Executive / Board / ARC as necessary.
- Escalating to the Executive / Board in a timely manner details of risks which cannot be mitigated or mitigated in a timely fashion which have a detrimental impact on the organisational aims and objectives.
- Reporting on risk assurances to the ARC when requested.

6.5. The Governance & Assurance Manager (or related role)

- Develop, document, maintain and promote the Risk Management Framework.
- Raise awareness of risk management, through communication of relevant processes, tools and techniques.
- Constructively challenge risks and mitigating actions.
- Raise awareness of sector and global risks, challenging the organisation's risk profile.
- Compile Strategic / Corporate risk information and prepare reports for the Executive, ARC and Board.

6.6. Operational Teams

Regularly reviewing the Operational Risk Register ensuring that risks for their areas of operation are clearly and accurately identified and scored, including identification of new and emerging risks and ensuring that they:

- Understand, accept and implement Risk Management processes.
- Report inefficient, unnecessary or unworkable controls.
- Report loss events to the Head of Governance, and near miss incidents / accidents to the Governance & Assurance Manager
- Co-operate with management on incident investigations.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

6.7. The Three lines of Defence

The roles and responsibilities outlined above aligns with IronOak's three lines of defence Model, which clarifies accountability for risk identification, oversight and independent assurance. This model ensures that risks are identified and recorded across every level, subject to appropriate oversight and independent review.

1 st Line of Defence	2 nd Line of Defence	Third Line of defence
Operational Management: - Housing Operations, - Asset Management & Repairs, - Finance & Income Management, - Development & Investment, - Neighbourhood and Resident Teams	Executive Leadership Team - Risk & Assurance, - Governance & Compliance, - Finance review and analysis, - Health & Safety Building Safety, - Policy owners, - Portfolio Quality Assurance Framework	Independent Audit and Assurance - Internal Audit (IronOak – independent, outsourced provider), - External Audit (statutory auditors), - Commissioned specialist independent reviewers (e.g., treasury advisors, rent valuation specialists, building safety consultants)

Table 1: Three Lines of Defence

The operation of the Three Lines of Defence is further supported by the Audit & Assurance Policy, which sets the process through which IronOak obtains assurance over the effectiveness of its activities.

6.8. Risk Assessment

IronOak has an established procedure and methodology for carrying out business risk assessments, which assists managers in identifying and mitigating key risks. The Risk Management Procedure at Section 3 provides further details in respect of this.

Executive and Senior Managers throughout the business are responsible for identifying, mitigating, and regularly reviewing their risks as outlined in either the corporate level or relevant operational level Risk Registers. The process of risk review involves all of IronOak's staff members.

Risk assessments are held on an ongoing basis, aligned to the corporate planning cycle, by Senior Managers, the Executive and the Governance and Assurance Manager (or related role) and when there are significant changes in corporate strategic thinking. Formal updates to risk assessments will take place when changes occur and as a minimum on a quarterly basis. The risk assessment process will identify those risks which have an impact on our ability to achieve objectives.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

It is the responsibility of managers to update their Risk Registers (or equivalent) regularly and provide updates upon the request of the Governance & Assurance Manager (or equivalent role).

6.9. Risk Appetite

When considering risk, it is important that everyone involved in identifying, evaluating, and mitigating risks is aware of the organisation's risk appetite as set by the Board. The Board sets its risk appetite through setting and understanding the overall organisation's objectives, reviewing the regulatory and legislative framework and the consideration of risk / reward and the extent to which risks should be mitigated against.

The Board uses a framework for understanding and agreeing their risk appetite. This is based on a model which assesses appetite levels from Entrepreneurial to averse. See Appendix 2.

Given the changing nature of the operating environment IronOak operates within, the Board assesses its appetite in relation to specific risks, keeping under review the impact the risks have collectively on its overall appetite. The risk appetite is reviewed annually by the Board and also when there are significant changes in internal and external factors.

For the avoidance of doubt, IronOak has identified the following risk appetite:

“Generally, IronOak takes a measured approach to risk mitigation expecting risks to be considered and managed effectively and within the Board's appetite as part of business-as-usual activities and when new opportunities arise. The Board, however, has no appetite to accept risk which could have a detrimental impact on the health, safety and wellbeing of our staff, customers and partners, this extends to the quality of care provided to our customers and the application of regulatory consumer standards which may cause serious detriment, for the avoidance of doubt this includes all aspects of regulatory compliance. In addition, the Board is wary of assuming risks that could potentially harm the organisation's reputation or financial stability. The Board expects robust mitigation will take place to limit financial exposures, protecting the long-term financial viability of the organisation.”

The Board has aligned the organisation's governance framework, Key Performance Indicators and financial requirements to its risk appetite. This is demonstrated through the following (for example):

- Property Compliance to be fully (100%) compliant with all statutory legal requirements such as gas safety and applies a window of tolerance where legally permissible.
- Regular review of the business plan and updating of stress testing scenarios.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

In addition to the above, the organisation's adopted governance framework ensures that the Board retains ownership of key strategic decisions and strategic direction and is aware of and where necessary approves exceptional items.

In reviewing risk mitigation, the Board and ARC both satisfy itself that planned risk treatments correlate with its risk appetite as outlined above. Further information on individual risk appetite is contained with the risk reports provided to the Board.

6.10. Risk Reporting

IronOak Homes will remain transparent at all times in the reporting of key risks and progress with mitigating strategies, through regular reporting to the Executive, Board and ARC, and externally to the Regulator where required.

The Risk Management Procedure provides further detail on the reporting of risk.

6.11. Conclusion

IronOak is committed to the effective management of risk. It is the requirement of all managers to implement reasonable measures to successfully mitigate risks to an acceptable / tolerated level, and where this is not achievable escalate significant risk exposures through relevant governance structures.

7. The Risk Management Procedure

The purpose of this procedure is to outline the requirements of how the business will successfully deliver risk management practices. It also promotes the value IronOak places on the effective management of risk and its correlation to good business practice.

The procedure applies to all Board Members, Co-optees, the Executive Leadership Team (ELT), Operations Management Team (OMT) and staff whether permanent, part-time, fixed term and casual employees of IronOak, and to any temporary staff, consultants or contractors, working on our behalf. It is the responsibility of any contracting manager within IronOak to make sure that all temporary staff, consultants and contractors are made aware of this procedure.

Roles and responsibilities of Board Members, Co-optees, the ELT, OMT and staff in respect of Risk Management are outlined in the Risk Policy above.

7.1. Risk Assessment Process

IronOak applies a systematic approach to risk assessment in accordance with current best practices. The result of the assessment is an output in the form of Risk Register which captures key risks, along with their information on related controls and assurance mechanisms. The risk assessment process is adopted for risks at a Strategic and Operational level. The objectives of the risk assessment are to:

- Identify, assess and prioritise key risks.
- Identify risk triggers.
- Establish the level of control currently applied.
- Confirm the assurances around control mechanisms.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- Outline further mitigation / management control required to reduce risk impact / likelihood; and
- Identify interdependent risks

Where risks and their triggers are identified, risk owners must ensure that appropriate controls and any further mitigation required are implemented to reach a desirable risk level that is within the organisation's risk appetite as set by the Board. The process of risk assessment is continuous with related Risk Registers updated regularly. The process is summarised in Figure 1 below, along with explanations of each of the key elements.

Process	Requirements
1. Identification	Risk identification is an ongoing process, and can be completed in a number of ways: • facilitated workshops which allows key stakeholders to discuss risks • regular discussion within peer groups and team meetings • review of business planning, performance monitoring, regulatory / legislative landscape • staff appraisals and 1-2-1s
2. Cause / Effect.	Identification of the root cause of the risk (triggers) and what effect if it materialises.
3. Current Controls	Review of the controls currently in place which mitigate the risk. A control is a process / measure which already exists to make sure the things we want to happen will happen, and the things we do not want to happen won't happen.
4. Assurance outcomes	Review of the variety of assurance mechanisms which support assessment of controls. Reviewing management reporting and performance indicators and independent assurance mechanisms.
5. Evaluate the Risk	Evaluation of the risk considering: • Impact – the effect to reputation, finance, management effort • Probability / Likelihood – the likelihood of the occurrence A 5x5 matrix has been developed (overleaf) to ensure risk significance can be identified.
6. Board Appetite Review	Review the residual risk outcomes against the Boards risk appetite, assess whether future actions are required to reduce the risk further to an acceptable level, increase the assurance over controls, or improve processes to achieve best practice.
7. Mitigating Actions	Document relevant actions. It could be decided if the risk exposure at the current controls level is satisfactory that the risk is tolerated without the need for further actions.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

8. Interdependency between Risks	Consider whether the risk is impacted by or impacts another risk, document how.
9. Progress Review	Regular review of progress with mitigation actions and the effect they have on the management of the risk should take place on a regular basis. This includes review of assurance mechanisms such as key operating performance indicators and independent assurance on systems and controls. Formal reporting to the Board through the ARC takes place quarterly for Corporate / Strategic risks. Management should escalate risks not contained within acceptable levels of risk appetite.

Figure 2: Risk Process

7.2. Risk Mitigation and Response

Once a risk has been identified, there a number of ways of controlling/ mitigating/ reducing it:

- Treat the risk - the most common way of managing risks and involves putting in place (or strengthening existing) systems and processes (internal controls) to control/mitigate the likelihood of the risk occurring and/or its impact.
- Tolerate the risk - accept the likelihood and consequences of the risk occurring if the risk is within IronOak's risk appetite.
- Transfer the risk – shift the risk, in whole or part, to a third party i.e. working in partnership with others or putting insurance in place to cap financial losses.
- Terminate the risk - withdrawing from an activity which causes the risk.

7.3. Documenting Risk

Risks facing IronOak are recorded on the relevant risk register which is controlled by the Governance and Assurance Manager (or related role):

- Strategic Risk Register – risks that arise from external factors or events, internal decisions or changes that could affect IronOak's ability to achieve its strategic objectives or long-term goals.
- Operational Risk Register - risks arise from the day-to-day operations and service delivery.

The format adopted is reflective of good practice and enables the effectiveness of existing and future controls to be measured along with the impact implemented controls have on risks. In addition, the format used allows for progress with ongoing actions to be monitored.

The format adopted includes the following:

- Risk Description
- Risk Owner
- Controls and strength of control
- Assurance mechanisms and strength of assurance

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- Residual / Net / Controlled Risk Score (Impact, Likelihood, Total)
- Assessment of Board Appetite
- Mitigating actions (action owner, completion date)
- Risk Triggers
- Interdependencies between Risks
- Progress/Comments

A detailed register and summary of the risks is provided to ARC with further summaries provided to the Board.

Guidance on assessment of risk, including risk triggers and individual areas of concern is documented in Appendix 3. The definition of risk triggers is provided Under section 4.

It is recommended that for operational risks a similar format is adopted which is supported by evidence of risk discussions. Documentation of risks and escalation of risks at a department level is the responsibility of the relevant Operational Manager. Risk Escalation must be considered when risks exceed agreed devolved risk appetite levels. To aid this escalation process at the end of each quarter there is a formal risk return provided by the Governance and Assurance Manager (Appendix 4) which details information on the risks, current risk score / profile and actions to manage / treat the risk to an acceptable level, rationale for changes to risk scores are also documented.

Further guidance on controls and assurance is documented in Appendix 5.

7.4. Risk Reporting

Regular risk analysis and reporting allows for effective monitoring and management of risk across the business.

The Strategic Risk Register is reviewed quarterly by the ELT and OMT, and a formal risk return provided by the ELT to the Governance & Assurance Manager or Company Secretary (Appendix 6). A report indicating progress on risk mitigation, together with a full Strategic Risk Return, is presented to the Executive, and for review and consideration at ARC meetings.

The Strategic Risk Register is also presented to the Board at least twice a year. Any exceptions or key risks which arise in the interim should be brought to the attention of the ELT, who will routinely update the ARC / Board as and when required.

It is the role of the Governance & Assurance Manager to monitor and analyse the progress of Strategic risks and mitigating actions and report progress accordingly to the Head of Governance (or related role) and the ELT. In addition, the Governance & Assurance Manager (or related role) uses sector and organisational knowledge and intelligence to challenge the risks which are reported, along with their progress.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

The Governance & Assurance Manager (or related role) also provides regular updates to the ARC on sector risks and issues as part of routine reporting. Reporting includes grouping of risks aligned to the organisation's strategic aims.

At an operational level it is the responsibility of the Operation Manager to undertake appropriate risk assessments for the areas they have responsibility for. Key risks which require escalation to an ELT member for consideration at a corporate level should be reported upwards through the normal line management structure. The Governance & Assurance Manager (or related role) will play a key role in encouraging appropriate risk consideration and reporting at all levels across the business.

Operation Managers may also be requested to attend ARC to provide assurance over departmental / operational risks.

In addition to risk reporting, the risk registers, and the quarterly updates the organisation has in place an annual assurance statement process whereby Operation Managers document their areas of responsibility and any concerns that they have in relation to achievement of objectives. The details contained in the assurance statements are followed up formally, with progress in managing concerns ascertained during the year.

In addition, any risk which has been identified which 'impacts' another department/function should be flagged by the Risk Owner (as defined in section 12), to the affected party.

7.5. Risk Ownership

A risk owner is identified for each operational and strategic risk to take principal responsibility for ensuring progress is being made at reducing/eliminating the risk and mitigations/controls are updated on the risk register. Risk owners are not necessarily expected to deliver the mitigations/controls, but ensure the identified actions are taken.

The risk owner will typically be a senior leader closely involved in delivering the area of the business where the risk has arisen to understand what mitigations/controls are possible and/or planned.

7.6. Risk Assessment Matrix

IronOak has adopted the following Risk Assessment Matrix (Risk Matrix) and the impact and likelihood that risks may have on the organisation:

Using the Risk Matrix provides a visual representation of risk information and assists management decision making, particularly when comparing the positioning of a range of risks. The Risk Matrix allows for:

- Consideration of the acceptable level of risk.
- A visual sense check on the risk scores applied to ensure they are proportionate when considered as a whole.
- Visual representation of movement between inherent to residual risk scores.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

IronOak uses the following 5 x 5 Risk Matrix (Figure 2) which assigns a rating to both likelihood and impact of individual risks.

Once the ratings are decided for the 'likelihood' and 'impact' of the inherent risk, the two ratings are multiplied together to arrive at the overall risk rating and level of risk (see Key below). This is repeated for the residual risk rating consider the additional controls/mitigations to be put in place.

The ratings for both the inherent and residual risks should be reviewed on a regular basis to reflect any changes as:

- Once delivered/completed, the 'Further controls/mitigations' are moved to the 'Existing controls/mitigations' column.
- New controls/mitigations may be added to the 'Further controls/mitigations' column to reduce the risk further.

Likelihood	>75%	Almost Certain	5	5	10	15	20	25
	50 - 75%	Likely	4	4	8	12	16	20
	25 - 50%	Possible	3	3	6	9	12	15
	5 - 25%	Unlikely	2	2	4	6	8	10
	0 - 5%	Remote	1	1	2	3	4	5
				1	2	3	4	5
				Low	Minor	Moderate	Major	Critical

Impact	Inability to service customers	No significant service impact or disruption up to 1 day.	Marginal reduction in performance, or disruption/failure. Inability to undertake key operational functions for 1-2 days	Unsatisfactory performance or disruption/failure and / or inability to undertake a number of key operational functions for 3-4 days	Service disrupted/ stopped for 5+ days	Ongoing failure to provide adequate service and / or inability to undertake key operational functions for more than 1 month.
	Health & Safety impact	Minor injuries not requiring professional medical treatment	Minor professional medical treatment required	Fails to prevent extensive, permanent injuries or long-term sickness	Fails to prevent death or causes permanent injuries or long-term sickness	Responsible for death

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

Legal & Regulatory Impact	Unlikely to lead to complaints, with minimal procedure breaches	Complaint/ litigation likely. Breaches in regulation or standards	Litigation expected, but defendable. Breaches of law punishable by fines.	Breaches of law punishable by imprisonment or significant fines	Litigation almost certain and difficult to defend
Reputational damage (Including media interest and exposure)	Low and variable level of customer complaint. Unlikely to cause adverse publicity	Minor adverse local publicity or regulator interest. Persistent but low level of customer complaints.	Minor adverse national publicity or significant adverse local publicity. Regulator interest. Loss of a major client. Significant levels of customer complaint. Significant levels of adverse publicity high level of administrative burden arising from monitoring.	Significant adverse national publicity, regulator, financier concern and high level of administrative burden arising from monitoring. Loss of major client/contract.	Perceived as a failing organisation requiring Regulator intervention, withdrawal of financiers and loss of support amongst a significant number of clients.
Environmental concerns	Environmental incident with no lasting detrimental effect	Short term (weeks) environmental or public health incident	Medium term (up to 1 year) major public health or environmental incident	Long term (1 year+) major public health or environmental incident	Permanent major environmental or public health damage
Financial impact (impact on I&E in any one Financial Yr)	Financial loss or overspend up to £10k	Financial loss or overspend between £10k and £50k	Financial loss or overspend between £50k and £250k > £2m < £5m Falls between 10 - 15% breaching covenants	Financial loss or overspend between £250k and £500k > £5m < £10m Falls below 10% breaching covenants	Uncontrollable financial loss or overspend above £500k > £10m and breaching covenants

Table 3: 5x 5 Risk Matrix

KEY		
1-5	Low Risk	Minimal impact, manageable with minimal resources
4-6	Medium Risk	Moderate impact, requires closer monitoring and some resources.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

9-12	High Risk	Significant potential impact, requires immediate attention and substantial resources.
15-25	Extreme Risk	Severe and imminent impact, requires urgent action and significant resources.

Table 4: Risk Categorisation

The assessment matrix is used at each stage of evaluating a risk, steps 5, and 9 within Figure 1.

ARC will review the above scoring methodology and definitions annually to ensure they remain appropriate and relevant.

IronOak has adopted the following scoring of the likelihood of risks occurring:

Likelihood	Score	Probability of risk occurring	Definition
Remote	1	5% and below	It could happen, but probably never will
Unlikely	2	5% to 25%	Slight possibility, but not expected
Possible	3	25% to 59%	Might occur, with a similar occurrence experienced by IronOak or within the sector
Likely	4	50% to 75%	Strong possibility, with similar occurrences often experienced by IronOak or within the sector
Almost certain	5	75% and above	Will almost certainly occur, with similar occurrences frequently experienced by IronOak or within the sector

Table 5: Scoring Methodology

ARC will review the above scoring methodology, including probability percentages and definitions annually to ensure they remain appropriate for IronOak.

7.7. Scoring Risks

A scoring methodology is used to assess and prioritise each risk to ensure consistency across the Operational and Strategic Risk Registers.

The scoring methodology identifies those risks by a system of colour coding. This allows for easy identification of the greatest threats should a risk crystallise for prioritisation and resources to be directed accordingly.

The Board has also set risk levels which would be deemed to be above the organisation's risk appetite and require priority action to mitigate. This level is set for risks with a controlled score above 10 (above the thick black line as documented in Figure 2). The Board and ARC review risks evaluate at this level in greater detail.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

The scoring of risks is on two specific factors:

- The likelihood of the risk occurring (see section 13.0) - the probability that the risk will crystallise and the risk event occur.
- The impact of the risk (see section 13.0) - the severity of the effects or consequences if the risk event was to crystallise. This may be related to a number of service areas, including service delivery, Health & Safety, reputation, regulation or finances.

8. Other Risk Matters

8.1. Risk Appetite

- Risk appetite is the amount of risk an organisation is prepared to accept, tolerate or be exposed to at any point in time.
- At IronOak, the Board has determined that risk appetite should align with strategic objectives and financial viability while ensuring compliance with regulatory requirements and safeguarding resident interests. Given the current Strategic Register and the risk appetite parameters set by the Board, IronOak adopts a differentiated risk appetite across key risks listed on the register.
- As and when new risks arise, IronOak will assess risk appetite in alignment with the differentiated risk model, ensuring that the approach remains relevant and responsive to the evolving risk landscape. The Board will review the risk appetite annually in conjunction with ELT, with ARC providing recommendations on risk appetite parameters for Board consideration.

8.2. Emerging Risks

- With the every-changing landscape of the social housing sector i.e. changing legislation and regulatory requirements, a cost of living crisis, new and/or re-emerging risks may be identified through the regular review of the Operational and Strategic Risk Registers and the operating environment more generally:
 - A new risk – previously unforeseen.
 - A re-emerging risk – a previously identified risk that changes to bring a new or different threat.
- When a new or re-emerging strategic risk is identified, it will be reported to ARC for approval to add it to the Strategic Risk Register, allowing for controls/mitigations to be put in place to prevent crystallisation.

8.3. Risk Triggers

- Risk triggers are predefined indicators or events that signal the potential emergence of or escalation of a risk, prompting proactive assessment, response and mitigation efforts by relevant stakeholders within the organisation.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

- When a new or emerging risk trigger that might crystallise into a risk is identified it will be reported to ELT and to ARC, allowing for controls / mitigations to be put in place to prevent crystallisation or control the risk.

8.4. Horizon Scanning

Horizon scanning involves looking to the medium and long-term to provide early warning of potential risks that may occur, allowing time for action to be taken before the risk materialises. This process helps to identify and react to emerging and re-emerging risks - it is not trying to predict the future. There is no standard definition for horizon scanning, with the Institute of Risk Management giving three possibilities:

- An organised and formal process of gathering, analysing and disseminating value-added information to support decision making.
- A systematic examination of information to identify potential threats, risks, emerging issues, and opportunities allowing for better preparedness and the incorporation of mitigation and exploitation into the policy-making process.
- Exploration of what the future might look like to understand uncertainties better and to analyse whether the organisation is adequately prepared for potential opportunities and threats.

Horizon scanning, therefore, works as an alert to identify early warning signals of emerging issues that may not have been considered before, allowing for quick and decisive action to be taken.

ARC will undertake an annual horizon scanning exercise with the Executive Leadership Team to pre-empt any emerging issues, using the RSH's annual Sector Risk Profile which sets out the main risks facing the social housing sector and some of the actions RPs should be taking to manage them.

8.5. Stress testing

The RSH expects Registered Providers, as part of their risk management approach, to stress test their plans against different scenarios. This requirement is set out in the Governance and Financial Viability Standard.

Stress testing goes beyond the standard assessment of risks but looks at combinations of economic and identified risks to allow the Board to understand the conditions that could lead to failure of the business.

Examples of stress testing at IronOak could be the combined risks of:

- Increased costs for delivering care and support services, with occupancy rates falling generating less income.
- Greater regulatory scrutiny requiring action, with an unstable management team to deliver with difficulty recruiting/retaining good calibre permanent staff.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

IronOak will revise and update its stress tested scenarios at least annually or sooner where material changes in legislation regulatory requirements or operational conditions necessitate a review

8.6. Monitoring and update of the Risk Management Framework

This Framework will be reviewed annually or sooner if organisation, legislative and/or regulatory changes occur that could impact on its content.

This Framework may be added to, varied or revoked, by agreement of the Board.

9. Related Policies & Documents

- NHF Code of Governance 202
- Governance and Financial Viability Standard 2015
- Board Terms of Reference
- Audit and Risk Committee Terms of Reference

Appendix 1 - Glossary of Terms

This glossary sets out definitions for the key terms used within the Risk Management Framework.

Term	Definition
Assurance	An evaluated opinion, based on evidence gained from review, on governance, risk management and internal controls
ARC	The Audit and Risk Committee
Control	A process, policy, practice, tool or structure used to manage risk
Crystallise	The moment a risk materialises and takes effect
ELT	Executive Leadership Team
Emerging risk	A new risk not previously identified
Horizon scanning	Identification of potential threats, risks, emerging issues and opportunities that allows for better preparedness
Impact	The probable effect should the risk occur
Inherent risk	The current risk level with the existing mitigations/controls in place (rather than the absence of any control)
Likelihood	The probability of the risk occurring
Mitigation	A strategy to prepare for and lessen the effects of risks
OMT	Operational Management Team
Operational risk	The risks associated with day-to-day operations and service delivery
Operational risk register	The register of the day-to-day risks
Re-emerging risk	A previously identified risk which changes to reflect a new or different risk
Residual risk	The remaining levels of risk after mitigations/controls have been put in place
Risk	The threat that an event or action could have an adverse affect
Risk averse	Unwilling to take risks or wanting to avoid risks as much as possible

Risk appetite	The amount of risk an organisation is prepared to accept, tolerate, or be exposed to at any point in time
Risk management	A logical and systematic method of identifying, analysing, assessing, treating, monitoring and communicating risks to minimise losses and maximise opportunities
Risk matrix	Used to define and visually display the level of risk by considering likelihood and impact
Risk mitigation	The process of reducing risk exposure by minimising its likelihood and impact
Risk owner	The person responsible for ensuring the risk is properly managed and monitored
Strategic risk	The risk of potential failures in strategic planning, possibly leading to non-achievement of core objectives
Strategic risk register	The register of the strategic risks
Stress testing	Testing how an organisation would cope in the face of a range of potential situations and/or combination of risks
Triggers	Predefined events or conditions that, when they occur, signal the need for a planned response to mitigate or address potential risks.

Appendix 2 - Risk Appetite Model

CORE RISK CONSIDERATIONS	Averse	Cautious	Medium	Open	Hungry
	Avoidance of risk and uncertainty is the key objective	Preference for very safe options that have a very low degree of inherent risk; acceptance that potential rewards therefore likely to be low	Preference for safe options that have a low degree of inherent risk; acceptance that potential rewards therefore likely to be limited	Preference for options which offer greater potential reward, willing to accept greater inherent risks	Preference for innovative options with highest potential rewards and inherent risks.
Financial	Avoidance of any financial loss is a key objective.	Only prepared to accept the possibility of very limited financial loss if essential	Prepared to accept the possibility of some limited financial loss	Prepared to invest for reward and minimise the possibility of financial loss by managing the risks to a tolerable level – clearly excluding risk of covenant breach	Prepared to invest for the best possible reward and accept the possibility of financial loss (although controls may be in place)
	Resources withdrawn from non-essential activities	Resources generally restricted to core operational targets	Resources allocated to deliver “housing plus EC” objectives	Resources allocated in order to capitalise on potential opportunities	Resources allocated without firm guarantee of return “investment capital” type approach
Legal & Regulatory	Not willing to risk challenge under any circumstances. No impact to regulation.	Only willing to risk challenge, where there is a robust legal opinion, that any such challenge would not succeed. No impact to regulation.	Only willing to risk challenge where we have legal opinion that we have a good case. Impact to regulation is limited and can be managed.	Willing to risk challenge where we have legal opinion that we have a reasonable case, and the rewards are worth the risk. Regulatory impact can be managed	Willing to risk challenger where the risk of losing is high but the rewards are similarly high.
Reputational	Zero appetite for any decisions that could lead to scrutiny of the group	Appetite for risk taking limited to those events where there is no chance of any significant impact	Appetite for risk taking limited to those events where there is little chance of any significant repercussion for the group should there be a failure	Appetite to take decisions with potential to expose the Group to additional scrutiny but only where appropriate steps have been taken to minimise exposure	Appetite to take decisions which are likely to bring scrutiny of the Group but where potential benefits outweigh the risks

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

Appendix 3 - Risk Assessment Guidance

1.1 Key Controls Dependency: What level of reliance is placed on the key controls?

Low	Medium	High
You place limited reliance on the control environment which has been established. There is a significant number of actions needed to be taken to improve the control environment.	You place an average level of reliance on the control environment which has been established. There are a number of actions needed to be taken to improve the control environment.	You place an average level of reliance on the control environment which has been established. There are few (if any) actions needed to be taken to improve the control environment.

1.2 Assurance Assessments: How strong are the assurance indicators both in design and in outcomes?

Design The depth, frequency of assurance	STRONG Comprehensive in scope	MODERATE Reasonable in scope	WEAK Limited in scope
Outcome The results of the assurance	STRONG Substantial Assurance	MODERATE Adequate Assurance	WEAK Inadequate Assurance

1.3 Trigger Assessment: What is the level of pass / fail of identified triggers, and the level to which they impact risk exposure ?

RAG	Definition
Red	Unacceptable levels of risk exposure - require immediate corrective action
Amber	Levels of risk exposure require constant active monitoring & measures to reduce exposure
Green	Acceptable levels of risk exposure – regular active monitoring measures

Appendix 4 - Operational Risk Return Form

Background
It is management’s responsibility to ensure risks relating to their individual departments are being managed effectively. The purpose of this update is to provide the Board with information and progress on managing departmental risks and to also identify progress with corporate risk mitigation. This process acts as an aide-memoir for to SMT to review their risk registers and provides a formal method for capturing the top department risks. It also gives Heads of Service the opportunity to escalate risks to a Strategic Level. SMT members are encouraged to collate their own department risks in a more detailed version than this return. Further guidance is contained in the organisation’s Risk Policy Framework. The documentation of risks allows for controls and future actions to be identified and managed in a coordinated way.
Requirements
You are requested to confirm that you have undertaken a review of risks and effectiveness of related controls for your department’s key risks. This includes informing the Governance and Assurance Officer of the top risks which are currently being managed within your department along with progress with intended actions. You are also requested to identify significant events, risks and areas of concern you feel need to be escalated to a strategic level, if any. A copy of the Parasol Q2 strategic risks is attached. In addition, where you have responsibility for managing one of the strategic risks you are required to provide an update on related controls, assurance mechanisms and their outcomes and progress with any mitigating actions. This should be completed within the new and refreshed SMT Strategic Risk Return specific to the risk(s) for which you are the nominated lead. Your assessment is to be returned to [name], Governance & Assurance Officer by [date].

1. Top Department Risks

In managing the areas for which I am responsible, I confirm that I have reviewed related risks and controls and confirm that controls which mitigate risks either continue to be effective or are receiving management attention. In completing this review I confirm that the following risks are those which cause me most concern in my area of responsibility and are being proactively managed as per the actions documented:

Top Department Risks		Potential Impact (1 - 5)	Likelihood (1 - 5)	Q1-Q2 risk changes (positive/negative)	Actions planned /in progress to manage risks with timescales for completion
1					
2					
3					
4					
5					

Impact Scores – 1 = Low 2 = Minor 3 = Moderate 4 = Major 5 = Critical

Likelihood Scores - . 1 = Remote 2 = Unlikely 3 = Possible 4 = Unlikely 5 = Almost certain.

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

2. Risk movement since QX

In reviewing my Q3 risks against risk reported in Q2, the following provides explanations of key changes.

Risks		Explanation of significant positive / negative movement
1		
2		
3		
4		
5		

3. Risk Flight Path		
In relation to the above, I assess the following areas to provide assurance that the risk has increased/decreased/ or has occurred or likely to occur (risk triggers):		
Risk	Increased/Decreased/ Occurred/Likely to Occur	Trigger events being reviewed
1.		
2.		
3.		
4.		
5.		

4. Significant Events / Areas of concern

I have detailed below significant events which I am aware of which have occurred in the last quarter or likely to occur in the near future which could have a detrimental impact to Parasol's reputation and or financial viability.

Examples of significant events could include significant budget overruns, areas of poor performance, significant quality or health and safety failures, potential areas of litigation, failures to comply with legislation / regulatory standards.

Significant events / Areas of concern

5. Risk Escalation

I have detailed below risks which I feel need to be escalated to a strategic level which currently do not appear on the strategic risk register – risks are documented in Appendix 1.

Escalated Risks

6. Corporate/Strategic Risk

I have reviewed the position of strategic risks which have been assigned to me either in my functional role or as a member of the strategic management team, I can confirm that progress is being made with risk mitigation. Updates have been provided in the spreadsheet, further details have been provided below.

Strategic Risks		Progress since Q2 – positive/adverse/no movement: Provide rationale for positive direction	Mitigations: Actions planned /in progress to manage risks with timescales for completion

Name:**Date:****Position:**

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

Risk Matrix – Probability and Impact Scores

Likelihood	>75%	Almost Certain	5	5	10	15	20	25
	50 - 75%	Likely	4	4	8	12	16	20
	25 - 50%	Possible	3	3	6	9	12	15
	5 - 25%	Unlikely	2	2	4	6	8	10
	0 - 5%	Remote	1	1	2	3	4	5
				1	2	3	4	5
				Low	Minor	Moderate	Major	Critical
		Inability to service customers		No significant service impact or disruption up to 1 day.	Marginal reduction in performance, or disruption/ failure. Inability to undertake key operational functions for 1-2 days	Unsatisfactory performance or disruption/failure and / or inability to undertake a number of key operational functions for 3-4 days	Service disrupted/ stopped for 5+ days	Ongoing failure to provide adequate service and / or inability to undertake key operational functions for more than 1 month.
		Health & Safety Impact		Minor injuries not requiring professional medical treatment	Minor professional medical treatment required	Fails to prevent extensive, permanent injuries or long term sickness	Fails to prevent death or causes permanent injuries or long-term sickness	Responsible for death
		Legal & Regulatory Impact		Unlikely to lead to complaints, with minimal procedure breaches	Complaint/ litigation likely. Breaches in regulation or standards	Litigation expected, but defensible. Breaches of law punishable by fines.	Breaches of law punishable by imprisonment or significant fines	Litigation almost certain and difficult to defend
		Reputational damage (Including media interest and exposure)		Low and variable level of customer complaint. Unlikely to cause adverse publicity	Minor adverse local publicity or regulator interest. Persistent but low level of customer complaints.	Minor adverse national publicity or significant adverse local publicity. Regulator interest. Loss of a major client. Significant levels of customer complaint. Significant levels of adverse publicity high level of administrative burden arising from monitoring.	Significant adverse national publicity, regulator, financier concern and high level of administrative burden arising from monitoring. Loss of major client/contract	Perceived as a failing organisation requiring Regulator intervention, withdrawal of financiers and loss of support amongst a significant number of clients.
		Environmental concerns		Environmental incident with no lasting detrimental effect	Short term (weeks) environmental or public health incident	Medium term (up to 1 year) major public health or environmental incident	Long term (1 year+) major public health or environmental incident	Permanent major environmental or public health damage
		Financial impact (impact on I&E in any one Financial Yr)		Financial loss or overspend up to £10k	Financial loss or overspend between £10k and £50k	Financial loss or overspend between £50k and £250k > £2m < £5m Falls between 10 - 15% breaching covenants	Financial loss or overspend between £250k and £500k > £5m < £10m Falls below 10% breaching covenants	Uncontrollable financial loss or overspend above £500k > £10m and breaching covenants

Appendix 3 - ELT Strategic Risk Evaluation form

Q1 STRATEGIC RISKS RETURN

RISK 1: **Limitations in the skills, vibrancy and effectiveness of the Executive, Board and Committee inhibits their ability to discharge their responsibilities.**

ELT Owner: Anthony Jenkins

Board Appetite	Averse
Within Appetite	Yes

KEY CONTROLS (*Controls which mitigate the risk*) **REVIEW TO ENSURE KEY CONTROLS CONTINUE TO BE RELEVANT**

1. Annual board-away day with focus on Parasol's future development.
2. Established Board and Executive with relevant skills and experience
3. (Annual) Board Appraisals by Chair; 6 month evaluation of Chair by Senior Independent Director
4. Board training and development
5. Routine Board Meetings
6. Agendas and papers for Board provide opportunities for discussion and challenge to the Executive with post-meeting evaluation questionnaires.
7. Exec appraisals, training and development (including 360 reviews)
8. Chair appraisal of the MD
9. Clear Board and committee governance structure
10. Board members interact with SMT and wider organisation

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

ASSURANCE (*Mechanisms that provide effectiveness over controls*)

REVIEW STATUS OF ASSURANCE AGAINST SOURCES AND UPDATE

Management	Date	Assurance Indicator	Independent	Date	Assurance Indicator
Board & Governance Committee papers	Mar' 24	Moderate/Strong	Internal Audit KPMG review of Financial Delegation Arrangements	Mar' 24	Moderate/Strong
Board Member Appraisal Outcomes	Mar' 24	Moderate/Strong			
New Chair appointed in Q2 of 2023	Mar' 24	Moderate/Strong	External Assurance Altair Review 2021	Mar' 24	Moderate/Strong
Review of processes & operations	Mar' 24	Moderate/Strong	Campbell Tickell Review 2022	Mar' 24	Moderate/Strong
			Campbell Tickell Review 2023	Mar' 24	Moderate/Strong

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

ACTIONS TO INCREASE KEY CONTROLS OR ASSURANCE **REVIEW PROGRESS AND UPDATE, ADD NEW ACTIONS WHERE RELEVANT**

ACTIONS	COMPLETED
1. End to end review by Governance & Assurance Officer includes practices, policies and procedures and Code of Governance Review 2. Board appraisals completed December/January 2023 to consider skills profiles, priorities for future Board recruitment and timetable for succession and transition planning. 3. Chair engagement factored into induction 4. Programme of Board visits with staff, residents and external stakeholders 5. 2 new independent board members of ARC 6. 1 new member of the Board 7. Post Board meeting on-line survey to capture views	1. By end of 2024 2. Ongoing 3. Completed by March 24 4. Ongoing 5. Completed 6. Completed Jan 24 7. On-going

TRIGGERS *(Events or conditions that would cause your risk to occur)* **REVIEW STATUS OF TRIGGER AGAINST SOURCES AND UPDATE PASS/FAIL/ACTION**

TRIGGER	Sources of Information	Pass/ Fail	Comments/Outlook/Corrective or Preventative Action	RAG
1. Change in MD/Chair without structured succession planning 2. One or more Board Members resign out of cycle 3. Board recommendations are outstanding more than 3 months 4. One strategic plan is made outside of the strategic cycle	Company Secretary and Board Minutes	1.Pass 2.Pass 3.Pass 4.Pass	No action at Present	

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

INTERDEPENDENCY BETWEEN RISKS (*Highlights other risks on the register that may be impacted by your risk*) **UPDATE FOR ADDITIONAL INTERDEPENDENCY**

WHAT RISK IS OR RISKS ARE IMPACTED?	HOW?
1. There is a regulatory downgrade as a result of non-compliance or an inability to demonstrate compliance.	The sound governance of Parasol is directly attributable to restoring our G1/V1 rating and ensuring that we do not have any further regulatory downgrades.

2. OVERALL RISK ASSESSMENT – COMPLETE THIS BOX BASED UPON ASSESSMENT OVERLEAF AND GUIDANCE IN 1.1-1.3 ABOVE

A. Control Dependency	Medium	
B. Assurance Indicator	Design: Moderate	Outcome: Strong
C. Risk Trigger Indicator	Green	

RESIDUAL RISK ASSESSMENT – UPDATE RISK SCORE

Residual Risk 2019/2020

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

	Probability	Impact	Total
Q1	1	4	4
Q2			
Q3			
Q4			

INTERNAL COMMENTS: **INSERT ADDITIONAL COMMENTS**

GUIDANCE ON ASSESSMENT OF RISK AND INDIVIDUAL AREAS OF RISK (CONTROLS, ASSURANCES, TRIGGERS)

2.1 Key Controls Dependency: What level of reliance is placed on the key controls?

Low	Medium	High
You place limited reliance on the control environment which has been established. There is a significant number of actions needed to be taken to improve the control environment.	You place an average level of reliance on the control environment which has been established. There are a number of actions needed to be taken to improve the control environment.	You place an average level of reliance on the control environment which has been established. There are few (if any) actions needed to be taken to improve the control environment.

1.2 Assurance Assessments: How strong are the assurance indicators both in design and in outcomes?

Design The depth, frequency of assurance	STRONG Comprehensive in scope	MODERATE Reasonable in scope	WEAK Limited in scope
Outcome The results of the assurance	STRONG Substantial Assurance	MODERATE Adequate Assurance	WEAK Inadequate Assurance

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

1.3 Trigger Assessment: What is the level of pass / fail of identified triggers, and the level to which they impact risk exposure ?

RAG	Definition
Red	Unacceptable levels of risk exposure - require immediate corrective action
Amber	Levels of risk exposure require constant active monitoring & measures to reduce exposure
Green	Acceptable levels of risk exposure – regular active monitoring measures

RESIDUAL RISK SCORING - PROBABILITY AND IMPACT MATRIX

Likelihood	>75%	Almost Certain	5	5	10	15	20	25
	50 - 75%	Likely	4	4	8	12	16	20
	25 - 50%	Possible	3	3	6	9	12	15
	5 - 25%	Unlikely	2	2	4	6	8	10
	0 - 5%	Remote	1	1	2	3	4	5
				1	2	3	4	5

Low

Minor

Moderate

Major

Critical

Impact

Inability to service customers	No significant service impact or disruption up to 1 day.	Marginal reduction in performance, or disruption/ failure. Inability to undertake key operational functions for 1-2 days	Unsatisfactory performance or disruption/failure and / or inability to undertake a number of key operational functions for 3-4 days	Service disrupted/ stopped for 5+ days	Ongoing failure to provide adequate service and / or inability to undertake key operational functions for more than 1 month.
Health & Safety impact	Minor injuries not requiring professional medical treatment	Minor professional medical treatment required	Fails to prevent extensive, permanent injuries or long-term sickness	Fails to prevent death or causes permanent injuries or long-term sickness	Responsible for death

Excellence ➤ Safety ➤ Sustainability ➤ Integrity

Legal & Regulatory Impact		Unlikely to lead to complaints, with minimal procedure breaches	Complaint/ litigation likely. Breaches in regulation or standards	Litigation expected, but defendable. Breaches of law punishable by fines.	Breaches of law punishable by imprisonment or significant fines	Litigation almost certain and difficult to defend
Reputational damage (Including media interest and exposure)		Low and variable level of customer complaint. Unlikely to cause adverse publicity	Minor adverse local publicity or regulator interest. Persistent but low level of customer complaints.	Minor adverse national publicity or significant adverse local publicity. Regulator interest. Loss of a major client. Significant levels of	Significant adverse national publicity, regulator, financier concern and high level of administrative burden arising from	Perceived as a failing organisation requiring Regulator intervention, withdrawal of financiers and
				customer complaint. Significant levels of adverse publicity high level of administrative burden arising from monitoring.	monitoring. Loss of major client/contract.	loss of support amongst a significant number of clients.
Environmental concerns		Environmental incident with no lasting detrimental effect	Short term (weeks) environmental or public health incident	Medium term (up to 1 year) major public health or environmental incident	Long term (1 year+) major public health or environmental incident	Permanent major environmental or public health damage
Financial impact (impact on I&E in any one Financial Yr)		Financial loss or overspend up to £10k	Financial loss or overspend between £10k and £50k	Financial loss or overspend between £50k and £250k > £2m < £5m Falls between 10 - 15% breaching covenants	Financial loss or overspend between £250k and £500k > £5m < £10m Falls below 10% breaching covenants	Uncontrollable financial loss or overspend above £500k > £10m and breaching covenants