RISK MANAGEMENT STRATEGY

Policy Classification: Key document

Status: Approved

Policy Lead:	Director of Finance & Corporate Services
Date Approved:	September 2019
Last Review Date:	December 2015
Review Due Date:	September 2022
Review Period:	3 years unless required earlier due to changes in the law, regulation, best practice or requirement of the Association

REFERENCE PAGE

Document Title:	Risk Management Strategy
Aim:	The resources available for managing risk are finite and so our aim is to achieve an optimum response to risk, prioritised in accordance with our evaluation of the risks.
Objective:	1 The Eildon Group will ensure that the highest standards of governance and partnership working are adhered to, including compliance with our regulatory frameworks
Scope of Policy:	All stakeholders
Nominated Officer:	Director of Finance & Corporate Services
Approval Source:	Board
Legal and Regulatory References:	
Document References:	• Supporting Treasury Management Policy • Sustainability Policy and 5 Year Plan.
Consultation Completed:	N/A
Risk Implications:	1- Existing policy, minimal change
Equalities Assessment:	All Eildon policies and key documents are developed with the clear objective of ensuring that they do not discriminate against any person and have negative impacts for equality groups. We will always welcome comments on the impact of a policy on particular groups of people in respect of, but not limited to, age, disability, gender reassignment, race, religion, sex or sexual orientation, being pregnant or on maternity leave and children’s rights and wellbeing.
Accessibility:	Accessible electronically/online and in print. All documents can be translated and made available in audio, braille and large print versions upon request.

Version Records		
Version	**Production/Changes Date**	**ARCOM Approval Date**
1	**February 2011**	**2 March 2011**
2	**November 2012**	**5 December 2012**
3	**November 2015**	**2 December 2015**
4	**September 2019**	**11 September 2019**

CONTENTS

1. OVERVIEW

1.1 Risk is defined as the uncertainty of outcome, whether positive opportunity or negative threat, of action and events with reference to the organisation's objectives Risk has to be assessed in respect of the combination of likelihood of something happening, and the impact that arises if it does happen.

1.2 The resources available for managing risk are finite and so our aim is to achieve an optimum response to risk, prioritised in accordance with our evaluation of the risks. We use the term 'risk appetite' to refer to the amount of risk which we are prepared to accept, tolerate, or be exposed to at any point in time.

1.3 Risk management is the process by which we:

- identify risks in relation to the achievement of Strategic and Departmental Objectives.
- Assess their relative likelihood and impact
- Respond to the risks identified, considering our assessment and risk
- Assess all tolerance of risk and the assurance levels of the controls
- Review and report on risks – to ensure the risk register is up to date, to gain assurance that responses are effective, and identify when further action is necessary

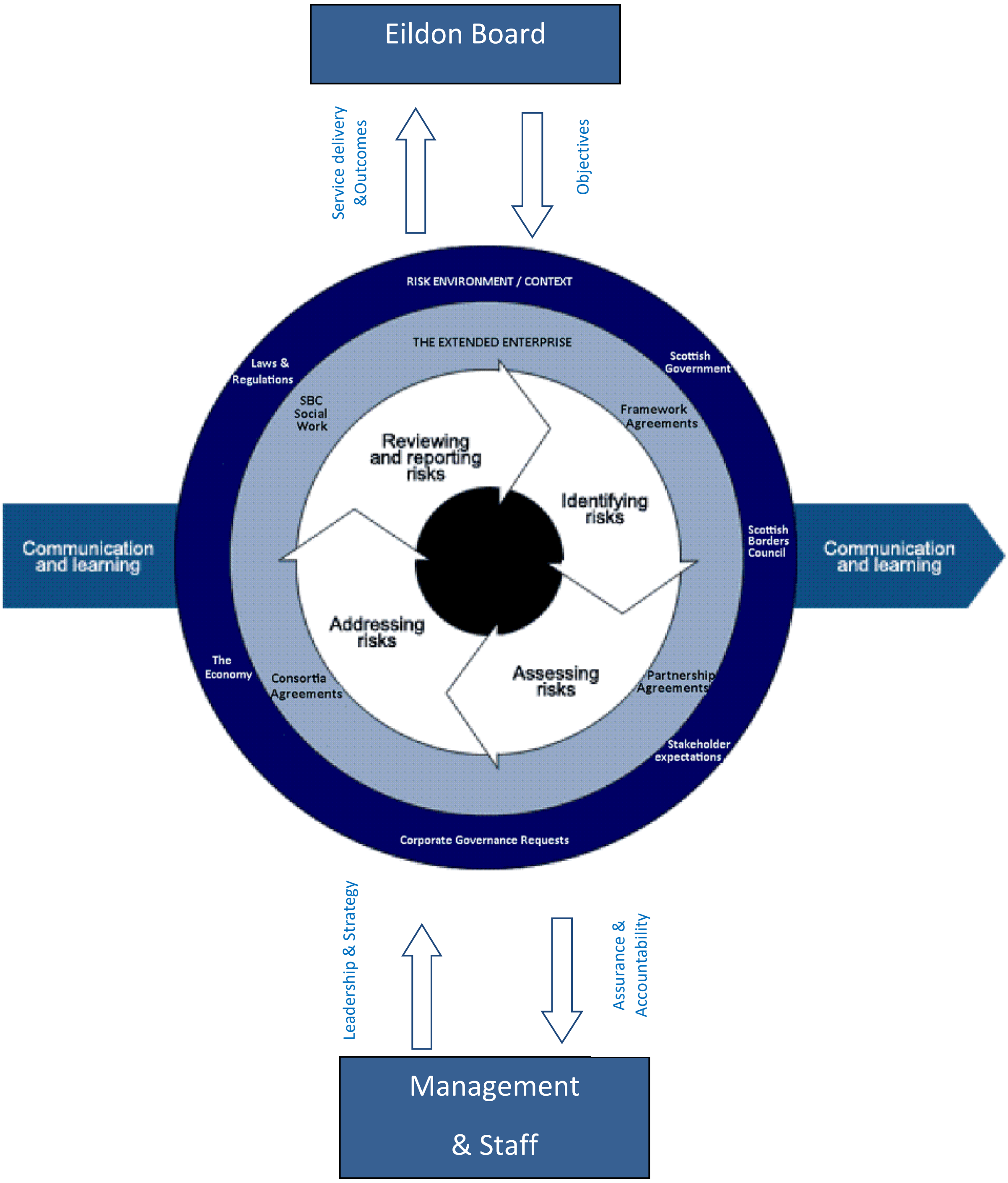
1.4 The goals of risk management are to:

- Take A Proactive Approach, Anticipating And Influencing Events Before They Happen
- Facilitate Better Informed Decision Making
- Protect And Promote The Organisation Reputation
- Improve Contingency Planning

1.5 The management of risk is not a linear process; rather it is the balancing of several interwoven elements which interact with each other. It is essential that the risk management process is intertwined with other operating activities and permeates the organisation's management.

This is illustrated by the Eildon Risk Management Model overleaf:

The Eildon Risk Management Model



Notes on the Model

- The management of risk is the balancing of several interwoven elements which interact with each other
- The Model dissects the core risk management process into elements for illustrative purposes, but in reality, they blend together
- The Model illustrates how the core risk management process is not isolated, but takes place in a context

2. Identifying Risks

2.1 Identifying risks is the first step in building the Risk Register. The process of identifying and defining risks establishes common understanding of the risks and therefore better capability to respond appropriately.

2.2 Twice a year a formal risk assessment exercise will take place. The Departmental staff will review in the context of the Departmental Objectives and the Executive Team the Corporate Strategic Objectives. The outputs of this process will be used to inform the Corporate Risk Register.

2.3 The Risk Register will be a live document with opportunities to update it on an ongoing basis, together with formal reviews - as set out in section 8.

2.4 When identifying and defining risks, the following guidelines should be followed:

- Risks should be related to the objectives
- A statement of risk should encompass the cause of the impact, and the impact/effect to the objectives which might arise
- Risks should be identified at a level where a specific impact can be identified

Understanding the most important "causes" 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.

2.5 It is easy to become confused when identifying risks so care should be taken to avoid:

- Getting into the labyrinth of stating the impact of other risk as risks themselves
- Stating risks that do not impact on the objectives
- Stating risks that are clearly well beyond the control of the company e.g. nuclear war
- Defining risks with statements which are simply the converse of objectives.

2.6 An example of a risk definition with causes, controls and actions is provided at **Annex 1.**

3. Assessing Risks

3.1 There are five important principles for assessing risks:

- Ensure that both likelihood and impact are considered for each risk
- Record the assessment of risk in a way which allows the identification of risk priorities
- Be clear about the difference between inherent (the risk before controls are considered) and residual (the risk after the controls are considered) risk
- Avoid confusing causes with risks
- Be clear about the assurance levels of the controls

3.2 For each risk an assessment should be made of the likelihood of it occurring and the relative impact if it does. The more clearly risks are defined at the identification stage, the more easily they can be assessed. Likelihood is the probability or chance of the risk occurring and impact is the probable effect on the Association if the risk occurs.

3.3 Some exposures are simpler to deal with than others. For example, financial risks are often easier to consider and assess than those associated with risks to the Association's reputation or its ability to provide a service. Where feasible, past events may provide a useful input to assess risks. While the risk identification and assessment is primarily aimed at those events that may occur within the planning period, managers should not ignore risks that are more long term.

3.4 All risks should be scored in terms of their likelihood and potential impact using the following five-point scale. The score for the likelihood and impact are calculated to give an overall risk assessment:

LIKELIHOOD			IMPACT	
5	**Almost Certain**		**5**	**Major**
4	**Likely**		**4**	**Significant**
3	**Possible**		**3**	**Moderate**
2	**Unlikely**		**2**	**Minor**
1	**Rare**		**1**	**Negligible**

3.5 Further guidance on assessing relative likelihood and impact is provided at **Annexes 2 & 3**. The information in these annexed forms part of the process for deciding when a risk should be escalated or reduced.

3.6 The impact descriptors are only an indication of the probable effect on the Eildon Group if the risk occurs; they are not hard and fast rules. It is essential that staff use their knowledge and judgement when deciding on the score for impact.

3.7 Each risk is assessed twice. Firstly the **'Before Controls'** risk, which is the exposure arising from a specific risk before any action has been taken to manage it. Secondly the **'After'** risk which is the exposure arising from a specific risk after action has been taken to manage it and assuming that the action is effective.

4. Addressing Risks

4.1 The purpose of addressing risks is to turn uncertainty to the organisation's benefit by constraining threats and taking advantage of opportunities.

4.2 The appropriate response to each risk will depend on its nature and the outcome of the risk assessment. The degree of attention required should be proportionate to the level of risk and the cost and benefits involved in any action taken to reduce the risk.

4.3 For each risk, the key activities designed to manage the exposure must be defined to support tracking and monitoring of the nature of the risk concerned. This must include both the risk at the time of the review – the controls in place at the time of the 'Before' assessment, and the action planned in the light of the 'After' assessment, including a target date for implementing the planned action.

4.4 There are four key aspects of addressing risk: [**Note the first three can run concurrently].**

1 **TOLERATE**: the exposure may be tolerable without any further action being taken. Even if it is not tolerable, ability to do anything about some risks may be limited, or the cost of taking any action may be disproportional to the potential benefit gained. In these cases the response may be to tolerate the existing level of risk.

2 **TREAT:** by far the greatest number of risks will be addressed in this way. The purpose of treatment is that whilst continuing within the organisation with the activity giving rise to the risk, action (control) is taken to constrain the risk to an acceptable level.

3 **TRANSFER:** for some risks the best response may be to transfer them. This might be done by conventional insurance, or it might be done by paying a third party to take the risk in another way.

4 **TERMINATE**: some risks will only be treatable, or confinable to acceptable levels, by terminating the activities.

5. Risk Appetite

5.1 The aim of the Risk Strategy is not to remove all risk but to recognise that some level of risk will always exist. Indeed, it is recognised that taking risks in a controlled manner is fundamental to innovation and the building of a "can do" culture. Risk appetite is the amount of risk that the organisation is prepared to accept, tolerate or be exposed to at any point in time.

5.2 Our risk appetite can be expressed as a boundary, above which we will not tolerate the level of risk and further actions must be taken:

The chart below sets out the possible scores when looking at a combination of 'Impact' and 'likelihood'.

IMPACT	Major - 5	15	19	22	24	25
	Significant - 4	10	14	18	21	23
	Moderate - 3	6	9	13	17	20
	Minor - 2	3	5	8	12	16
	Negligible -1	1	2	4	7	11
		Rare - 1	Unlikely - 2	Possibly - 3	Likely - 4	Almost Certain - 5
		LIKELIHOOD				

	Key	
Severe	20-25	Unacceptable level of risk exposure which requires immediate corrective action to be taken.
Major	15-19	Unacceptable level of risk exposure which requires constant active monitoring, and measures to be put in place to reduce exposure.
Moderate	11-14	Acceptable level of risk exposure subject to regular active monitoring measures.
Minor	7-10	Acceptable level of risk subject to regular passive monitoring measures.
Insignificant	1-6	Acceptable level of risk subject to periodic passive monitoring measures.

Everything that scores 14 or under is acceptable and anything that scores 15 and above isn't.

5.3 The risk appetite is monitored by the Before and After risk assessment figures. Generally, we will wish to manage closely all residual risks scoring 15+ and will not wish to tolerate risks scoring 19+.

5.4 An organisation's risk appetite is not necessarily static. The Board may vary the amount of risk which it is prepared to take depending on the circumstances.

5.5 The Board has agreed to focus on monitoring of risks with a score of 15 or more and have delegated to the executive team for the review and monitoring of the whole register, and those risks scoring less than 15.

6. Risk Roles and Responsibilities

Board

The Board has responsibility for ensuring that the Association fulfils the aims and objectives set out in its Rules, and for promoting the efficient and effective use of staff resources. The Board shall demonstrate high standards of corporate governance at all times, including using the Audit & Risk Committee (ARCOM) to help address the key risks facing the Association.

Only strategic risks with a residual level of 15 or more on the register will be submitted to the Board.

Audit & Risk Committee (ARCOM)

The ARCOM is responsible for ensuring proper arrangements exist for risk management and internal control. It considers and advises the Board on:

- The strategic processes and policies for risk, control and governance including the content of the Statement of Internal Control, prior to endorsement by the Board
- The promotion, co-ordination and monitoring of risk management activities, including regular review of the corporate risk profile
- Assurances relating to the adequacy and effectiveness of risk control and governance

The ARCOM will be provided with:

- A biannual report summarising any significant changes to the Risk Register
- An annual report on the executive team review of the risk processes.
- A triennial report on the executive team review of the risk strategy.

Chief Executive (CEO)

The CEO is personally responsible for safeguarding the funds for which he/she has charge; for ensuring propriety and regularity in the handling of those funds; and for the day-to-day operations and management of the Association.

In managing risk, the CEO is responsible for ensuring that:

- A system of risk management is maintained to inform decisions on financial and operational planning and to assist in achieving objectives and targets
- The board are involved in the risk management system
- A risk register is maintained

This includes:

- Setting and communicating the Risk Strategy
- Providing leadership over the risk process
- Regularly reviewing the Risk Register
- Conducting an annual review of the effectiveness of the system of internal control.

Executive Team (ET)
The ET works with managers in delegating effective risk management in their areas of responsibility.

They are responsible for delegating the management of risks to identified staff. They are also responsible for developing and implementing the process and maintaining the risk register document. The Director of Finance and Corporate Services will be responsible for ensuring the Risk Register is kept up to date and submitted to the ARCOM.

Managers
Everyone with a line or project management role is responsible for assessing and communicating risks within their sphere of responsibility, including judging when a risk should be considered for inclusion in the Risk Register.

Risk owners
Risk owners are responsible for ensuring that each risk assigned to her/him is managed and monitored over time.

All staff
Whilst this strategy document sets out defined processes for managing risk, successful risk management can only be accomplished on a day to day basis by staff at all levels through their working practices; it does not simply lie inert in corporate policies and management structures.

Risk management is the responsibility of every member of staff and virtually everyone has a role in carrying out appropriate risk management by supporting risk identification and assessment, and designing and implementing risk responses. This will be achieved through core briefings, team meetings and one to one sessions, etc.

Internal Audit

The Internal Audit function plays a key role in evaluating the effectiveness of, and recommending improvements to, the risk management process. This is based on the systematic review and evaluation of the policies, procedures and operations in place to:

- Establish, and monitor the achievement of, the organisation's objectives
- Identify, assess and manage the risks to achieving the organisation's objectives
- Advise on, formulate, and evaluate policy
- Ensure the economical, effective and efficient use of resources
- Ensure compliance with established policies (including behavioural and ethical expectations), procedures, laws and regulations
- Safeguard assets and interests from losses of all kinds, including fraud, irregularity or corruption
- Ensure the integrity and reliability of information

In addition, Internal Audit aims to add value through:

- Supporting the identification of risks and the development of processes and procedures to assess and effectively respond to risks
- The identification and recommendation of potential process improvements
- The provision of advice to manage risks in developing systems projects, and procedures
- The provision of best practice advice to all sections of the association; and encouraging best practice and engendering continuous improvement.

7. Risk Register and Risk Maps

7.1 The Risk Register is the list of risk by department showing the controls and the proposed action. It informs the reader by:

- Facilitating the identification of risk priorities
- Capturing the reasons for decisions made about what is and is not tolerable exposure
- Recording the way in which it is decided to address risk
- Allowing those concerned with risk management to see the overall risk profile and how their areas of responsibility fit into it
- Facilitating the review and monitoring of risks

7.2 Heat Maps are simply the lists with only the before and after risks scores. This data shows the number of risks by score.

8. Reviewing and Reporting Risks

8.1 The management of risks must be reviewed and reported on for two reasons:

- To monitor whether or not the risk profile is changing
- To gain assurance that risk management is effective, and to identify when further action is necessary

8.2 The review mechanism consists of:

- An annual review of the processes and the Strategy itself by the Executive Team (ET) which is then signed off by Audit & Risk Committee (ARCOM)
- A bi-annual revaluation of the existing risks and the identification of new risks

8.3 The reporting mechanism consists of:

- The reporting firstly to the ARCOM and then the Board the results of the bi-annual revaluation
- The ET annually confirming, via the Internal Statement of Control, that to the best of their knowledge and belief the risks have been regularly identified and assessed, and key risks have been effectively managed

8.4 Should circumstances dictate it the revaluating and reporting time spans in 8.2 and 8.3 above will be shortened. Similarly, new risk can be added to the register at any time.

8.5 The risk management processes described in this document operates in the context of a wider assurance framework within the organisation, as shown at **Annex 4**.

8.6 In addition to the mechanism of monitoring and reviewing the Risk Register, the Group has the following other internal control and assurance mechanisms:

- The Outsourced Internal Audit firm also provides a written report every 3 years to the Board outlining their opinion of the overall adequacy and effectiveness of the organisation's risk management processes, including their relevant strengths and weaknesses.

- As a part of its work, the Association's External Auditors examine and comment on the Board's Statement of Internal Control.

9. Communication and Learning

9.1 Communication and learning is not a distinct stage in the management of risk; rather it is something which runs through the whole process. The identification of new risks or changes in risk is itself dependent on communication.

9.2 Externally, the organisation needs to maintain a good network of communications with relevant contacts and sources of information to facilitate identification of changes which affect the Association's Risk Register.

9.3 Internally it is important to embed risk management, ensuring that all staff understand, in a way appropriate and relevant to their role, what the risk strategy is and their role in managing risks and keeping the Risk Register up to date.

9.4 To do this team meetings are used to promote increased awareness and understanding of corporate and operational risks and risk management performance issues and training is given.

9.5 Communication with partner organisations about risk issues is essential to ensure understanding of respective risk priorities. Arrangements for doing this with specific partners are outlined in the following section.

10. The Extended Enterprise

10.1 The Group is self-contained however it has to be recognised that there are partner organisations which create a number of interdependencies which give rise to additional risks which need to be managed.

10.2 Specific arrangements to manage external interdependencies include:

- Contract Agreements with other RSLs such as the Repairs and Maintenance contract with Waverley.
- Formal Contracts with SBC for the provision of care services to our projects.
- Offers of HAG from the Scottish Government More Homes Division for our Development Programme.
- Agency Contracts e.g. SBC (Care and Repair) and development for SBHA.

11. Environment and Context

11.1 The Group's activities are impacted by the macro economy, the housing markets, and wider cultural and social factors relating to housing. We also need to be sensitive to stakeholder expectations, in the housing and related sectors, and amongst our end users - the beneficiaries of our affordable housing activities.

11.2 Our relationship with the Scottish Government and Scottish Borders Council is fundamental to our purpose. We explicitly consider risk management in policy making, aiming to include a proportionate and wide-ranging consideration of risk prior to policy proposals.

12. REVIEW

This policy should be reviewed within three years unless required earlier due to changes in the law, regulation, best practice or requirements of the Association.

Annex 1 - Example of with Causes and Controls

Risk Ref	Risk Title	Cause & Effect	Before Controls Score	Risk Control	Assurance Level	After Risk Score
IT 1	IT FAILURE - Total or partial failure of the IT System with a down time greater than 24 Hours	Cause : - Hardware failure (Servers/infrastructure) - Phone line/communication failure - Business Continuity event - Cloud Failure - Lack of or limited monitoring of the IT systems health Effect : - Staff unable to access system / Lost business days - Organisation cannot communicate effectively - Payroll delayed - Loss of housing data - Unable to reconcile accounts - Key data information and communications lost. - Reputational damage - Potential local media interest,	I = 5 L = 3 22	Constant monitoring of the IT systems health Control Owner: Robert McDade	Adequate	I = 2 L = 3 8
IT 1	IT FAILURE - Total or partial failure of the IT System with a down time greater than 24 Hours	Cause : - Hardware failure (Servers/infrastructure) - Phone line/communication failure - Business Continuity event - Cloud Failure - Lack of or limited monitoring of the IT systems health Effect : - Staff unable to access system / Lost business days - Organisation cannot communicate effectively - Payroll delayed - Loss of housing data - Unable to reconcile accounts - Key data information and communications lost. - Reputational damage - Potential local media interest,	I = 5 L = 3 22	Ensure continual access system / reduced lost business days Control Owner: Robert McDade	Substantial	I = 2 L = 3 8
IT 1	IT FAILURE - Total or partial failure of the IT System with a down time greater than 24 Hours	Cause : - Hardware failure (Servers/infrastructure) - Phone line/communication failure - Business Continuity event - Cloud Failure - Lack of or limited monitoring of the IT systems health Effect : - Staff unable to access system / Lost business days - Organisation cannot communicate effectively - Payroll delayed - Loss of housing data - Unable to reconcile accounts - Key data information and communications lost. - Reputational damage - Potential local media interest,	I = 5 L = 3 22	Reduced likelihood of Cyber Attack Control Owner: Robert McDade	Substantial	I = 2 L = 3 8
IT 1	IT FAILURE - Total or partial failure of the IT System with a down time greater than 24 Hours	Cause : - Hardware failure (Servers/infrastructure) - Phone line/communication failure - Business Continuity event - Cloud Failure - Lack of or limited monitoring of the IT systems health Effect : - Staff unable to access system / Lost business days - Organisation cannot communicate effectively	I = 5 L = 3 22	Cloud Security Control Owner: Robert McDade	Substantial	I = 2 L = 3 8

Risk Ref	Risk Title	Cause & Effect	Before Controls Score	Risk Control	Assurance Level	After Risk Score
		- Payroll delayed - Loss of housing data - Unable to reconcile accounts - Key data information and communications lost. - Reputational damage - Potential local media interest,				
IT 1	IT FAILURE - Total or partial failure of the IT System with a down time greater than 24 Hours	Cause : - Hardware failure (Servers/infrastructure) - Phone line/communication failure - Business Continuity event - Cloud Failure - Lack of or limited monitoring of the IT systems health Effect : - Staff unable to access system / Lost business days - Organisation cannot communicate effectively - Payroll delayed - Loss of housing data - Unable to reconcile accounts - Key data information and communications lost. - Reputational damage - Potential local media interest,	I = 5 L = 3 22	Business Continuity event Control Owner: Robert McDade	Adequate	I = 2 L = 3 8

Examples of Action Plans

Risk Ref	Risk Title	Action Required	To be implemented by
Operational Risk / Care Services (ALD)			
Care (ALD) 1	INCOME & BUDGETS- Fail to effectively balance budgets and income	SDS approach to be developed	17 Jun 2020
Care (ALD) 2	MANAGING THE WORKFORCE - Inability to manage our staffing resources to ensure they are sufficient to deliver the service	Checklist for line-managers as discussed with HR to reduce sickness absence in the service, working collaboratively to train senior team to	05 Jul 2019
Care (ALD) 4	CARE PLAN - Fail to ensure that care plans are appropriate and effective	All care plans and risk assessment information to be moved onto StoriiCare (as	30 Jun 2019
Care (ALD) 5	PROPERTY SAFETY: Fail to ensure all properties meet the appropriate safety standards	Core task mapping to be completed for SSW role and for SW role.	02 Aug 2019
Operational Risk / Corporate Services			
Corp 1	COMMUNICATIONS - Inability to effectively market Eildon Housing and manage our brand	Communications strategy to be developed	07 Dec 2018
Operational Risk / Human Resources			
HO 5	PEOPLE PLANNING - Staffing resources and skills are not aligned to the needs and future	Defined Succession plans	28 Nov 2019

Annex 2 - Assessment and Evaluation of Risks

Up until the impact descriptors this is good stuff – the impact descriptors need to be more relevant to Eildon.

Assessment of risk

For each risk identified, an assessment should be made of the likelihood of it occurring and the relative impact if it does. The more clearly risks are defined at the identification stage; the more easily they can be assessed. Likelihood is the probability or chance of the risk occurring and impact is the probable effect on the Corporation if the risk occurs.

Some exposures are simpler to deal with than others. For example, financial risks are often easier to consider and assess than those associated with risks to the Association's reputation or its ability to provide a service. Where feasible, past events may provide a useful input to assess risks. While the risk identification and assessment is primarily aimed at those events that may occur within the planning period, managers should not ignore risks that are more long term.

Evaluation of risk

When evaluating risk, the following criteria need to be considered:

- financial and value for money issues
- human resource issues – capacity, relations and others
- service delivery and quality of service issues
- public concern, trust or confidence issues
- degree and nature of risks to the public
- reversibility or otherwise of realisation of risks
- the quality or reliability of evidence surrounding the risk
- the impact of the risk on us (including its reputation), stakeholders and the public
- defensibility of realisation of the risk

All risks should be scored in terms of their likelihood and potential impact using the following five-point scale. The score for the likelihood and impact are calculated to give an overall risk assessment:

Likelihood		Impact	
5	Almost Certain	5	Major
4	Likely	4	Significant
3	Possible	3	Moderate
2	Unlikely	2	Minor
1	Rare	1	Negligible

The impact descriptors are only an indication of the probable effect on the Association if the risk occurs; they are not hard and fast rules. It is essential that staff use their knowledge and judgement when deciding on the score for impact.
In particular when assessing financial impact, staff and Board Members should take account of the potential cumulative effect of what might be considered smaller sums on the overall resource constraints of the organisation. For example, a number of individual overruns on development schemes could have a cumulative and significant impact on the overall viability of the development programme.

In addition, staff and Board members should consider different financial thresholds for risks that impact on the impact assessments descriptors below.

Likelihood descriptors

Almost certain: Likelihood greater than 75%

- Very likely
- The event is expected to occur in most circumstances
- There could be a history of regular occurrences at the Association i.e. on an annual basis
- If new event, likelihood of occurrence regarded as almost inevitable (3.1)

Likely: Likelihood greater than 50%

- There is a strong possibility the event or risk will occur (more than 2:1)
- There may be a history of frequent occurrences at the Association
- Everyone with knowledge of issues in this area knows this could happen
- No or little effective measures to reduce likelihood can be and/or have been taken
- Will probably occur in most circumstances

Possible: Likelihood between 10% and 50%

- The event might occur at some time
- There could be a history of casual occurrence at the Association
- Most of the team know that the risk might occur
- Measures that reduce likelihood have been taken but are not fully effective

Unlikely: Likelihood between 1% and 10%

- Not expected, but there’s a slight possibility it could occur at some time
- Some of the team consider this a risk that might occur
- Conditions exist for this loss to occur
- Probably requires more than two coincident events

Rare: Likelihood less than 1% likelihood

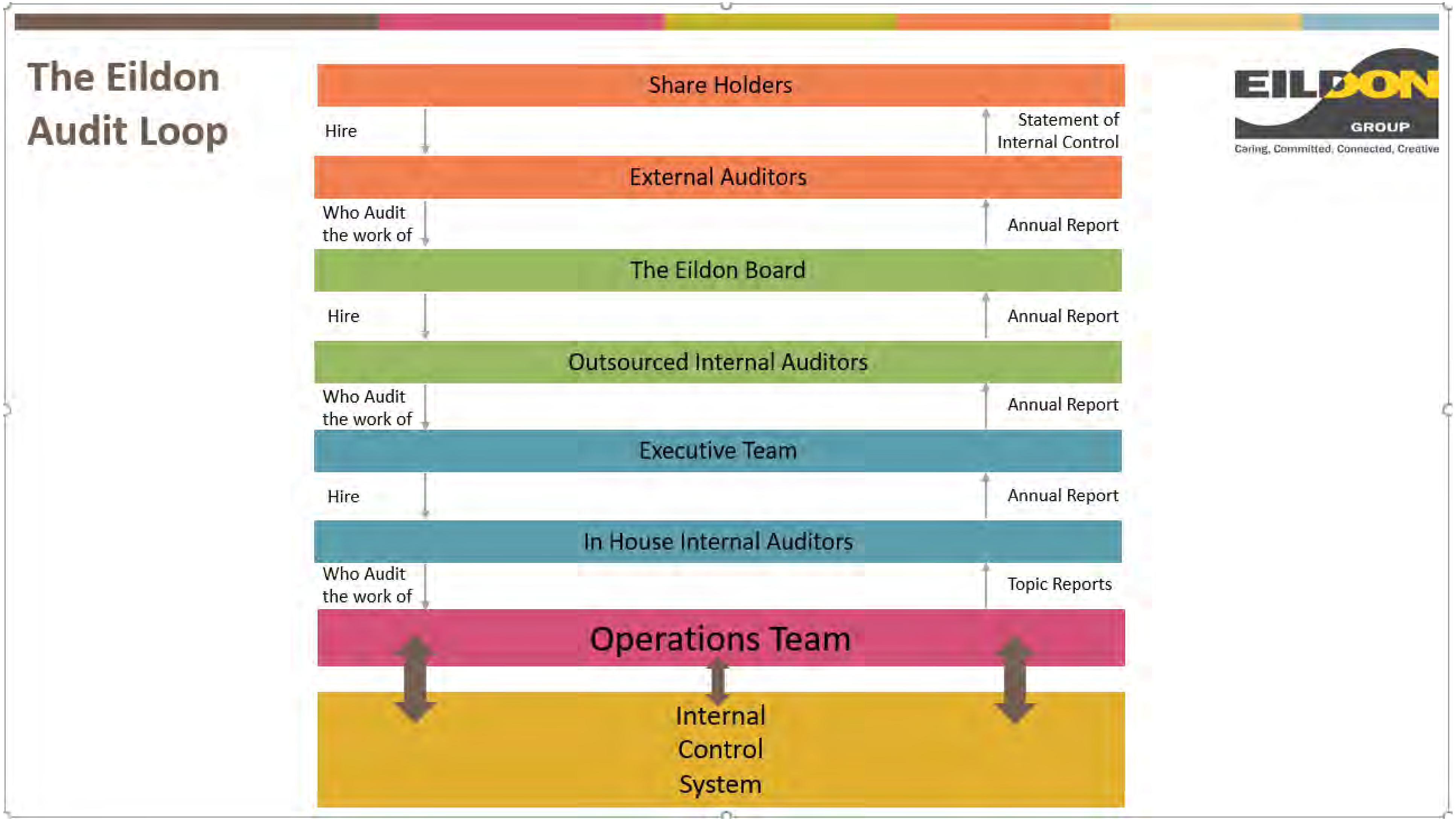
- Highly unlikely, but it may occur in exceptional circumstances
- It could happen, but probably never will
- No experience of a similar failure
- If it has happened, sufficient controls now in place

Annex 3 - Impact Descriptors

Rating	Rating Scale	Safety	Reputation	Media Attitude	Scottish Housing Regulator	Legal Action	Staff	Criminal	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.	Unsupported threat of legal action	Minimal effect on staff.	High control standards maintained and recognised.	Between0 - £1,000	No or little change to regulation in recent history / near future	Negligible effect on service quality
MINOR	2	Small risk of minor injury. H&S policy not regularly reviewed.	Some external stakeholders aware of the problem, but impact on is minimal.	Negative general Housing Association article of which EHA is mentioned	Verbal comments received	Legal action with limited potential for decision against	[potential for additional workloads intruding into normal non-working time	Attempted unsuccessful access to operational systems; minor operational information leaked or compromise d	Between £1,000 – and £10,000	Limited recent or anticipated changes	Marginally impaired – slight adjustment to service delivery required
MODERATE	3	High risk of injury, possibly serious. H&S standard s insufficie nt / poor training.	A number of Stakeholders are aware and impacted by problems	Critical article in Press or TV. Public criticism from industry body	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 into operational systems	Between £10,000 – and £50,000	Modest changes recently or anticipated	Service quality impaired changes in service delivery required to maintain quality
SIGNIFICANT	4	Serious risk or injury possibly leading to loss of life. H&S investigat	Significant disruption and or cost to Stakeholders third parties.	Story in multiple media outlets and / or national TV main news over	Multiple or repeat governance failings results in SHR intervention	Law suit against 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	Between £50,000 – and £300,000	Potential intervention by lead regulator. Significant changes to industry	Significant reduction in service quality experienced

Rating	Rating Scale	Safety	Reputation	Media Attitude	Scottish Housing Regulator	Legal Action	Staff	Criminal	Direct Loss	Regulatory / Industry Status	Service Quality
		ion resulting in investigation and loss of revenue.		more than one day				compromised			
MAJOR	**5**	Potential to cause one or a number of fatalities. H&S breech causing serious fine, investigation, legal fees and possible stop notice	Stakeholders; Third parties suffer major or loss or cost.	Government or comparable political repercussions. Loss of confidence by public	Action brought against EHA for significant governance failings forced merger	Action brought against EHA for significant breach	Deaths and / or major effect on staff lives	Major successful fraud; prosecution brought against EHA and Exec for significant failure; systems totally compromised	Over £300,000	Major complex changes to industry intervention on behalf of the Lead regulator	Complete failure of services

Annex 4 - The Eildon Audit Loop



The Eildon Audit Loop

Share Holders

Hire

Statement of Internal Control

External Auditors

Who Audit the work of

Annual Report

The Eildon Board

Hire

Annual Report

Outsourced Internal Auditors

Who Audit the work of

Annual Report

Executive Team

Hire

Annual Report

In House Internal Auditors

Who Audit the work of

Topic Reports

Operations Team

Internal Control System

Annex 5 - Glossary of Key Terms

Assurance An evaluated opinion, based on evidence gained from review, on the organisation’s governance, risk management and internal control framework.

Exposure The consequences, as a combination of impact and likelihood, which may be experienced by the organisation if a specific risks realised.

Impact The probable effect on the Corporation if the risk occurs.

Inherent risk The exposure arising from a specific risk before any action has been taken to manage it.

Likelihood The probability or chance of the risk occurring.

Residual risk The exposure arising from a specific risk after action has been taken to manage it and making the assumption that the action is effective.

Risk uncertainty Of outcome, whether positive opportunity or negative threat, of action and events. It is the combination of likelihood and impact.

Risk appetite The amount of risk that an organisation is prepared to accept, tolerate, or be exposed to at any point in time.

Risk assessment The evaluation of risk with regard to the impact if the risk is realised, and the likelihood of the risk being realised.

Risk management All the processes involved identifying, assessing and judging risks, assigning ownership, taking actions to mitigate or anticipate them, and monitoring and reviewing progress.

Risk register - The documented and prioritised overall assessment of the range of specific risks faced by the Association.