Governance 1.X

RISK MANAGEMENT POLICY

Reviewed by: M Nadin
Reviewed on: August 2019
Next Review: August 22

1. Policy Statement

1.1 Scottish Veterans Residences (SVR) (the organisation) is committed to developing and implementing Risk Management processes that will identify, assess, manage and review risks that may threaten the delivery of key priorities, objectives and values.

1.2 The purpose of this policy and its associated procedures is to make clear the standards and accountabilities for the management of risk within the organisation to ensure that:

- Statutory, regulatory and legal obligations are met;
- Residents, tenants, staff, assets and the reputation of the organisation are protected;
- Standardised tools for the management of risk are provided;
- Training and support for staff in the management of risk is available; and
- Assurance can be provided to the Governing Body regarding the effective implementation of this policy.

2 Scope

This policy applies to all areas and activities of the organisation and to all individuals employed by it including contractors, volunteers, bank, locum and agency staff.

3 Framework

3.1 The framework for Risk Management provides a defined approach that will be implemented across the organisation. Detailed instructions are provided in the associated procedural documents.

3.2 The Chief Executive shall approve all procedural documents associated with this policy and any amendments to such documents, and is responsible for ensuring that such documents are compliant with this policy.

3.3 Types of Risk

Strategic Risks

3.3.1 Strategic Risks relate to the strategic objectives of the organisation.

They are identified by the Executive Team[1], Governing Body Sub-Committee, or are risks that have been escalated by a Residence Manager. They are recorded on the Strategic Risk Register and reported on in the Governing Body Assurance Framework/Balanced Scorecard.

Project Risks

3.3.2 Project Risks relate to a project's objectives and are generally expressed in terms of anything that may impact on cost, time or quality.

3.3.3 Project Risks are managed in the same way as other risks within the organisation in that risk registers will be maintained, reporting schedules, and escalation thresholds to appropriate stakeholders will be defined, and the route of assurance to the Governing Body is made clear. These details will be included in a Project Initiation Document.

Operational Risks

3.3.4 Operational Risks relate to the day to day activity of the organisation and may be anything that could impact on the achievement of objectives at an operational level. The subject of Operational Risk will be classified as:

- **Quality (Q)** – Risks that may impact on the safety or effectiveness of support or housing service delivery, experience for Residents and Tenants and the ability to manage quality (governance).

- **People and resources (PR)** – Risks that may impact on staffing, security and welfare of people.

- **Information and communication technology (ICT)** – Risks that may impact on IT infrastructure systems and resources and their ability to support the organisation in pursuit of its objectives.

- **Finance and efficiency (FE)** – Risks that may impact on income, expenditure, procurement, business continuity, value for money and protection of assets.

- **Regulation and compliance (RC)** – Risks that may impact on legal/regulatory requirements including but not limited to the Office of the Scottish Charity Regulator, Scottish Housing Regulator, Care Inspectorate, Financial Instructions, fraud, claims, Information Governance and Duty of Candour.

[1] Executive Team consists of the Chief Executive, Depute Chief Executive, Head of External Relations and Company Secretary.

- **Reputation (R)** – Risks that may impact on the reputation of organisation derived from internal or external issues.

- **Health and Safety (HS)** – Risks related to the assessments of hazards under the associated Health and Safety Policy. Records of hazards and their assessment form a part of the day to day activities of the organisation and will be available to all staff members.

3.3.5 Each Residence and Head Office will maintain a Risk Register. Risks for which the Residence Manager lacks the resources to mitigate the risk adequately, are to be reported to the Executive Team.

3.4 Risk Management Process

3.4.1 The process for Risk Management consists of 4 steps to identify, assess, manage and review risks. These are described in greater detail in the associated Risk Management Procedure. Standards that apply to each step are:

Identifying the Risk

3.4.2 All staff have a role to play in identifying risk which may arise from a wide range of internal and external sources as outlined at Annex C.

3.4.3 All Residences, Head Office and General Housing will have a nominated Risk Lead who will ensure a Register of Risks which may impact on the achievement of objectives is maintained.

Assessing the Risk

3.4.4 All staff must follow the standardised approach to Risk Assessment outlined in the associated Risk Management Procedure. The use of consistent vocabulary assists the effective management of risk and standardises our corporate approach. To support staff in consistency of vocabulary, a glossary of terms is included in Annex E to this policy.

3.4.5 All risks will be scored and graded according to likelihood and consequence using the organisation's Risk Assessment Matrix at Annex B.

Managing the Risk

3.4.6 Once a risk has been assessed staff will decide how to respond based on the organisation's Risk Appetite and the

resources available. Responses can be a mix of four main actions; Transfer, Tolerate, Treat, or Terminate. These options are described in greater detail in the associated Risk Management Procedure.

3.4.7 New Operational Risks with a current score of 15 (RED) or above will be presented to the Chief Executive for approval within one month of being identified.

Reviewing the Risk

3.4.8 All risks with a current score of 15 (RED) or above must be reviewed each month. Those with a current score of 12 or below (AMBER and GREEN) will be reviewed each quarter. The review will be recorded on the appropriate risk register by the Risk Owner, supported by the Risk Manager. The review is to ensure that the Risk Assessment represents the current situation taking into account any changes to the context, deterioration of Controls, implementation of actions or change in Risk Appetite.

3.4.9 When the current score of a risk reaches the target score it will be reviewed by the Risk Owner with a view to accepting the risk. Any risk that reaches a score where it has been accepted must be reviewed every six months to ensure there has not been any significant change in the context of the risk or in the effectiveness or the efficiency of the controls.

3.4.10 Strategic Risks will be reviewed by the Governing Body at each of its meetings.

3.5 <u>Risk Escalation</u>

3.5.1 An integral part of effective risk management is ensuring risks are escalated within the organisation to ensure that appropriate action and prioritisation of resources can take place. Risks are escalated according to the progress in reaching the target score (further details can be found in the Risk Management Procedure). Where a risk cannot be managed to an acceptable risk level within the available resource or in an agreed timescale, the risk must be escalated.

3.5.2 For Operational Risks, the maximum time a risk will be 'Treated' by a Risk Owner is 12 months. At this time any risk that has not reached an acceptable risk level must be escalated to the Executive Team or Governing Body Sub-Committee for consideration.

3.6 Risk Reporting

Risk data will be used to produce reports to facilitate scrutiny and provide assurance regarding the implementation of this policy. Reports may be adapted at any time to suit the requirements of the Governing Body or its Sub-Committees. Generally, reports are scheduled as detailed below:

Table 1: Scheduled Risk Reports

Report	Schedule	Content
Residence and Head Office Risk Register	Monthly	Risks pertaining to individual Residences or Head Office. Residence and Head Office risks with a current score of 12 or above, or those for which the Residence Manager/Executive lack the resources to mitigate the risk adequately' are to be reported to the SMT. They are reviewed monthly at the SMT meeting.
Strategic Risk Register	Quarterly	Strategic Risks relate to the strategic objectives of the organisation. They are identified by the Executive Team. Strategic Risks are reported to the Governing Body. They are reviewed at Governing Body meetings.

3.7 Risk Assurance

3.7.1 The Governing Body needs to be aware of the current state of progress with regard to its strategic objectives including threats to achievement (Risk), controls that have been put in place and actions that are planned.

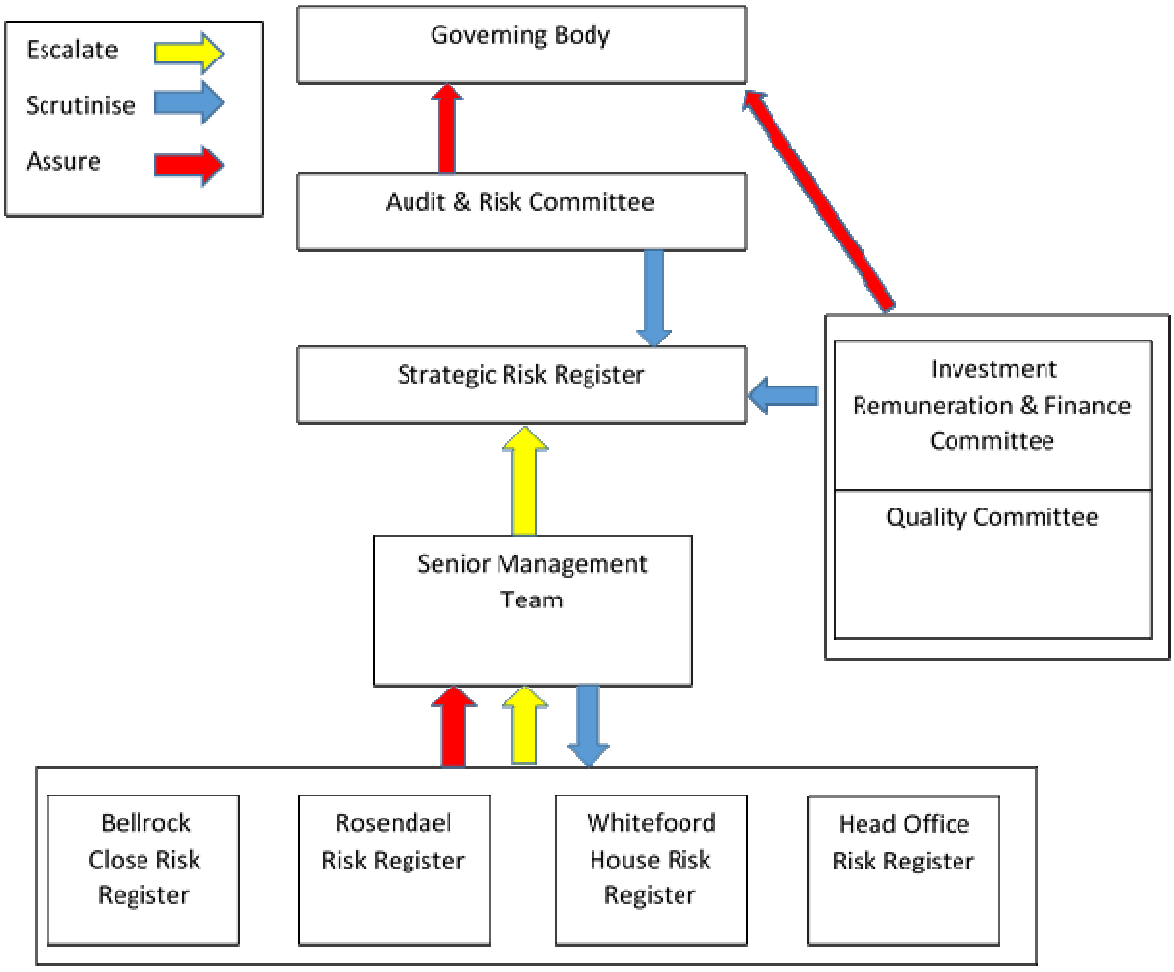
3.7.2 The resource of the Governing Body is finite; members cannot be present at every meeting to oversee every transaction and therefore the responsibility for carrying out operational activity falls to the Senior Management Team. As a result the Governing Body requires regular assurance that the organisation is working to achieve strategic objectives in the expected way with the expected outcomes.

3.7.3 The Governing Body will decide on the most appropriate source of assurance dependent on the importance of the subject in question and its risk appetite in relation to it. Assurances will enable the Governing Body to have a greater degree of trust in that assurance giving greater confidence about the likely achievement of strategic objectives and providing a sound basis for decision-making.

3.7.4 The sum of assurances received by the Governing Body constitutes the Governing Body Assurance Framework.

Figure 1 shows how this process is enacted within the organisation.

Figure 1. Risk Reporting, Escalation and Assurance



3.8. Risk Appetite

Risk Appetite identifies the amount of risk the Governing Body is willing to accept in pursuit of its objectives. The Governing Body will agree a statement against each objective which sets out their Risk Appetite and quantifies the level of tolerance it is prepared to accept. Risk Appetite statements and tolerance limits must be used to derive acceptable target scores for risk. The current Governing Body Risk Appetite Statement is found at Annex D.

4. Roles and Responsibilities

The Governing Body has overall responsibility for Risk Management within the organisation. Certain aspects of this are delegated to committees and

individuals as follows:

4.1 Audit and Risk Committee In relation to the management of risk the members of the Audit and Risk Committee will:

4.1.1 Ensure that an annual review of the risk management process is undertaken and it provides assurance to the Governing Body based on outcome; and

4.1.2 Seek further assurance on the management of specific areas of risk as required by the Governing Body.

4.2 Chief Executive

4.2.1 The Chief Executive (CEO), as the Chief Risk Officer, is accountable for the organisation's risk management framework and ensuring that this operates effectively.

4.2.2 The CEO must seek assurance from the systems and processes for risk management and ensure these meet statutory, regulatory and legal requirements.

4.3 Senior Management Team

4.3.1 As members of the Senior Management Team (SMT) all Executives and Residence Managers are responsible for overseeing a programme of risk management for the areas of responsibility/Residence.

4.3.2 This will include the provision of assurance to the Audit and Risk Committee on the management of operational risk, approval and review of operational risks identified within their areas of responsibility, ownership of escalated risks and consideration of strategic risk and assurance for inclusion on the GBAF.

4.4 Executives

4.4.1 All Executives are responsible for overseeing a programme of risk management activities for their areas of responsibility, in accordance with this policy.

4.4.2 This will include the provision of assurance to the SMT on the management of risk within their area of responsibility approval and review of risks, ownership of risks and consideration of operational risk for escalation to the SMT.

4.5 Residence Management Teams Residence Management Teams will have day to day accountability for the management of all risks relating to their Residence. They are responsible for:

4.5.1 Ensuring that risk management processes are in place and functioning appropriately within their Residence.

4.5.2 Reviewing risks that are more than 2 years old to confirm their validity.

4.5.3 This will include the provision of assurance to the SMT on the management of risk reported on the Residence Risk Register, approval and review of Residence risks, ownership of risks and consideration of operational risk for escalation to the SMT.

4.6 Risk Lead Each Residence will nominate a Risk Lead who is responsible for:

4.6.1 Ensuring that staff within the Residence are able to identify risks and how to report them to the Risk Lead.

4.6.2 Ensuring risk assessments are completed for risks identified within the Residence and documented according to this policy.

4.6.3 Ensuring that Residence staff implement action plans to reduce risk according to this policy.

4.6.4 Ensuring that risks are monitored and reviewed appropriately and that the risk register is updated to reflect progress and is accepted when the target score is met.

4.7 Risk Owner

4.7.1 All risks will have an identified Risk Owner who is responsible for ensuring that relevant risks are managed appropriately. This includes:

a. The ongoing action, monitoring of controls and scheduled review with update of the risk.

b. Reporting on the overall status of the risk including the need for escalation.

4.8 All Staff All staff have a responsibility for the identification, reporting, assessment and management of risks and to ensure they make themselves aware of and comply with the organisation's policies and procedures.

5. Implementation and Monitoring

5.1 Implementation

5.1.1 This policy will be available on the organisation's shared drive and will also be disseminated through the organisation's management structure.

5.1.2 Appropriate training will be provided for all roles with risk management responsibility.

5.2 Monitoring Annex A provides full details on how the policy will be monitored within the organisation.

6. Associated Policy and Procedure

Health and Safety Policy

Risk Management Procedure

Annexes:

A. Monitoring Matrix.
B. Risk Assessment Matrix.
C. Sources of Risk.
D. Governing Body Risk Appetite Statement.
E. Glossary of Terms.

Annex A – Monitoring Matrix

Monitoring of Implementation	Monitoring Lead	Reported to:	Monitoring Process	Monitoring Frequency
Identifying Risk – All Residences, Head Office and General Housing will have a nominated Risk Lead.	Business Information Analyst	Chief Executive	Review of Risk Registers	Monthly
Assessing Risk – All risks will be scored and graded according to likelihood and consequence using SVR's Risk Assessment Matrix.	Business Information Analyst	Senior Management Team	Review Risk Registers	Monthly
Managing Risk – New operational risks with a current score of 15 (RED) or above will be presented to the Chief Executive for approval within one month of identification.	Business Information Analyst	Chief Executive	Review of Risk Registers	Monthly
Reviewing Risk – All operational risks with a current score of 15 (RED) or above must be reviewed each month.	Business Information Analyst	Chief Executive	Review Risk Registers	Monthly
Reviewing Risk – All risks with a current score of 12 or below will be reviewed quarterly.	Business Information Analyst	Senior Management Team	Review Risk Registers	Quarterly
Reviewing Risk – When the current score of a risk reaches the target score it must be reviewed by the Risk Owner with a view to accepting the risk.	Business Information Analyst	Senior Management Team	Review Risk Registers	Monthly
Reviewing Risk – Strategic Risks will be recorded on the Strategic Risk Register, reviewed by the appropriate Sub-Committee and reported quarterly to the Governing Body.	Business Information Analyst	Governing Body	Board Assurance Framework	Quarterly
Risk Escalation – Where a risk cannot be managed to an acceptable risk level within the available resource or in an agreed timescale it is to be escalated to the SMT for consideration.	Business Information Analyst	SMT	Review Risk Registers	Monthly
Risk Management Process – Review of SVR's process undertaken as part of internal audit.	Chief Executive	Audit & Risk Committee	Internal audit review	Annual

Annex B – Risk Assessment Matrix

Risk scores are calculated by multiplying the likelihood of the Risk occurring by the consequence:

	Consequence				
Likelihood	(1) Insignificant	(2) Minor	(3) Moderate	(4) Severe	(5) Catastrophic
(5) Highly Likely	5	10	15	20	25
(4) Likely	4	8	12	16	20
(3) Possible	3	6	9	12	15
(2) Unlikely	2	4	6	8	10
(1) Rare	1	2	3	4	5

Risk likelihood will be assessed according to the following criteria:

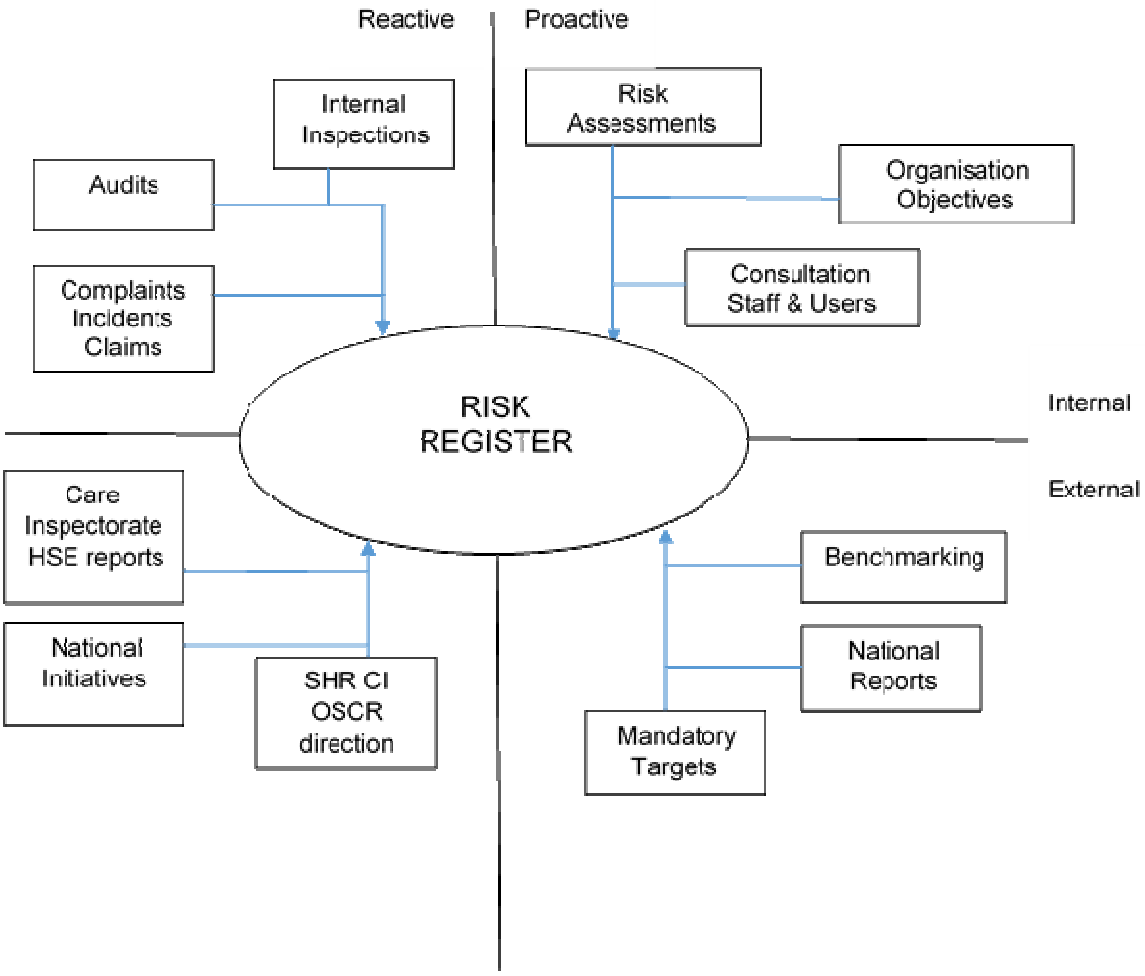
Descriptor	Rare 1	Unlikely 2	Possible 3	Likely 4	Highly Likely 5
Frequency	May not occur for several years (>5)	Could occur at least once in a 5 year period	Could occur at least once a year	Could occur at least once in 6 months	Could occur at least once per month
Probability	<1%	1% - 24%	25% - 50%	51% - 85%	>85%

Risk Consequence will be assessed according to the following criteria:

Risk Category	Insignificant 1	Minor 2	Moderate 3	Severe 4	Catastrophic 5
Quality	Potential for peripheral element of support or service may be suboptimal	Overall service may be suboptimal	Quality of service may significantly reduce effectiveness	Potential failure to meet internal standards Potential non-compliance with national standards	Potential for totally unacceptable level of service or quality Potential repeated failure to meet internal standards Potential gross failure to meet national standards
Compliance & Regulatory	None or minimal impact or breach of guidance or statutory duty or national standards	Single failure to meet guidance or national standards	Repeated failure to meet guidance or national standards Single breach of statutory duty Demanding external rec'dations	Non-compliance with national standards with significant risk to residents/ tenants if unresolved Multiple breaches in statutory duty – enforcement action	Totally unacceptable level of quality of service Multiple breaches in statutory duty Prosecution
Financial	Loss or overspend of £5k or less Risk of claims remote	Loss or overspend of >£5k but no more than £10k Claim <£10k	Loss or overspend of >£10k but no more than £25k Claim between £10k and £25k	Loss or overspend of >£25k but no more than £50k Claim between £25k and £50k	Loss or overspend of >£50k Claim >£50k
Reputation	Rumours with potential for public concern	Local media coverage Elements of public expectation not being met	Local media coverage Short term reduction in public confidence	National media coverage Long term reduction in public confidence	Ongoing National media coverage Total loss of public confidence

Risk Category	Insignificant 1	Minor 2	Moderate 3	Severe 4	Catastrophic 5
Resource & People	Minor schedule slippage but no effect on achievability of objectives Short term low staffing level temporarily reduces service quality (<1 day)	Significant schedule slippage but no other effect on achievability of objectives Low staffing level that reduces service quality	Some non-key objectives not achievable Late delivery of key objective or service due to lack of staff Unsafe staffing level or competence (>1 day)	Uncertain delivery of key objectives or service due to lack of staff. Unsafe staffing level or competence (>5 days) Loss of key staff	Non-delivery of key objectives or service Non-delivery of key objective/ service due to lack of staff Ongoing unsafe staffing levels or competence Loss of several staff
ICT	Potential loss of service or interruption of <12 hours Absolute certainty that no adverse effect can arise even if a data breach may occur	Potential loss of service or interruption of 12 - 24 hours Potential minor adverse effect from data breach	Potential loss of service or interruption of 24 - 48 hours Potentially some adverse effect from data breach, e.g. embarrassm't from release of info into public domain	Potential loss of service or interruption of 2 - 7 days Loss of named protected characteristics or resident's support plan into public domain	Potential loss of service or interruption of >7 days Potentially suffering financial loss from a data breach
Health Safety & Environment	Minimal injury requiring minimal intervention of treatment No time of work No or minimal impact or breach of guidance/ statutory duty Minimal or no impact on the environment	Minimal injury requiring first aid treatment Requiring <7 days off work Breach of statutory duty (no harm caused) Minor impact on environment	Moderate injury requiring professional intervention RIDDOR reportable requiring 7–14 days off work Single breach in statutory duty (harm caused) Moderate impact on environment	Major injuries or long term incapacity/ disability Requiring >14 days Multiple breaches in statutory duty (harm caused) Major impact on environment	Event may lead directly to death Multiple permanent injuries or irreversible health effects Catastrophic impact on environment

Annex C – Sources of Risk



Privacy Impact Assessments

The purpose of the Privacy Impact Assessment (PIA) is to ensure that privacy risks are minimised while allowing the aims of the project to be met whenever possible. Risks can be identified and addressed at an early stage by analysing how the proposed uses of personal information and technology will work in practice. This analysis can be te4sted by consulting with people who will be working on, or affected by, the project. These can be risks to the individuals affected in terms of the potential for damage or distress. There will also be corporate risks to the organisation carrying out the project, such as the financial and reputational impact of a data breach. Projects with higher risk levels and which are more intrusive are likely to have a higher impact on privacy.

Annex D – Governing Body Risk Appetite Statement

The Governing Body expects SVR's staff to identify risks that may impact on the achievement of objectives. The Risk Appetite Statement clarifies the level of such risk that is acceptable to the Governing Body and translates this into acceptable risk scores (its tolerance) that allow freedom for managers and executives to use their discretion when they implement controls to manage risk.

The acceptable levels of risk are:

Risk Appetite	Definition
No Appetite	The Governing Body is not prepared to accept uncertainty of outcomes at this level.
Low Appetite	The Governing Body accepts that a low level of uncertainty exists but expects that risks are managed to a level that may not substantially impede the ability to achieve objectives.
Moderate Appetite	The Governing Body accepts a moderate level of uncertainty but expects that risks are managed to a level that may only delay or disrupt progress of objectives but will not stop achievement.
High Appetite	The Governing Body accepts a high level of uncertainty and expects that risks may only be managed to a level that may significantly impede the ability to achieve objectives.

Operational risks are to be considered under the following categories:

- Quality
- People and resources
- Information and communication technology
- Finance and efficiency
- Regulation and compliance
- Reputation
- Health and Safety

Each category of risk may have various sub-categories, for example Quality risks may be risks relating to safety, effectiveness or user experience.

Acceptable risk scores are based on SVR's Risk Assessment Matrix and the Governing Body has specified the maximum acceptable target score for each sub-category of risk.

Annex E – Glossary of Terms

Definitions provide an agreed vocabulary that supports consistent communication and quality of assessment. The following definitions will be applied within SVR to the management of risk:

Control: The mitigating action that is implemented to reduce the likelihood or consequence of a risk occurring. Controls must be monitored to provide assurance that they continue to mitigate risk to an acceptable level.

Current Score: The level of risk when the likelihood and consequence are assessed taking into consideration the effect of controls.

Governing Body Assurance Framework: The key source of evidence that links strategic objectives to risks and assurances, and the main tool that the Governing Body will use in discharging its overall responsibility for internal control.

Initial Score: The level of risk when the likelihood and consequence are assessed before any control activities are applied (sometimes called the inherent risk).

Issue: An event that has already happened, was not planned and requires management action. It is not a risk.

Operational Risk: An uncertain event or condition that may affect the achievement of operational objectives, often impacting on the day to day activity of SVR.

Project Risk: An uncertain event or condition that if it occurs, has a positive or negative effect on a project's objectives related to cost, time and quality.

Risk: A risk is a future uncertain event or set of events that if it were to occur, will have an effect on the achievement of business, project or programme objectives. A risk can be a threat or an opportunity to the objectives of SVR.

Risk Appetite: A narrative statement that clarifies the amount of risk the Governing Body is willing to accept in pursuit of its objectives.

Risk Assessment: The process by which SVR identifies, describes, evaluates and estimates (quantitatively and qualitatively) a risk.

Risk Escalation: Where a risk cannot be managed to an acceptable level risk level within the available resource or in an agreed timescale then the risk must be escalated to a higher level for review. This may result in a change of risk owner if the review shows that the risk cannot be managed appropriately at the lower level.

Risk Lead: The member of SVR staff responsible for the day to day administration of risk management procedures. The risk lead supports the risk owner in the management and review of risk.

Risk Level: After a risk has been assessed the scores may be:

- Red Risk – a high risk with a current score of 15, 16, 20 or 25.
- Amber Risk – a significant risk with a current score of 5 (L1 x C5), 6, 8, 9, 10 or 12.

- Green Risk – a low risk with a current score of 1, 2, 3, 4 or 5 (L5 x C1).

Risk Management: The systematic application of processes and procedures that SVR puts in place to ensure it identifies, assesses, prioritises and takes action to manage risks to ensure it continues to deliver its objectives. Risk management is an ongoing process that must form part of everyday management activity. Risk must be manages so far as is reasonably practical.

Risk Owner: The member of SVR staff responsible for the management of individual risks.

Risk Proximity: The estimate of when the risk is likely to occur. Identifying risk proximity helps to prioritise risk and identify the appropriate response.

Risk Register: A log of all risks that may threaten SVR's success in achieving its declared aims and objectives. It provides a structure for collating information that enables risks to be identified and quantified. It also helps to provide a framework to make decisions about how each risk must be managed. It can be used as a prioritising tool to guide the allocation of resources and can be linked to the business planning process.

Risk Status: The current management status of a risk and is determined by the approach taken in terms of Terminate, Tolerate, Transfer or Treat.

Risk Tolerance: A translation of risk appetite into a range of risk scores that the Governing Body is willing to accept.

Strategic Risk: A risk that may threaten strategic objectives of SVR. This type of risk will be owned by an Executive.

Strategic Risk Register: A register of strategic risks owned by Executives and reviewed by the Governing Body.

Target Score: The level of risk when the likelihood and consequence are assessed taking into consideration the appetite for risk in pursuit of objectives.

Terminate Risk: An option for managing a risk where the risk owner decides that the current level of risk is too high and will not proceed with the activity that has led to the risk.

Tolerate Risk: An option for managing a risk where the risk owner decides that the current level of risk is in line with the agreed risk appetite/tolerance and accepts that no further action is required other than managing controls and quarterly review.

Transfer Risk: An option for managing a risk where the risk owner decides that the current level of risk is too high and transfers the risk to another owner, e.g. purchase an insurance policy so that if the risk materialises the financial loss is covered, or transfer a service to another accountable owner.

Treat Risk: An option for managing a risk where the risk owner decides that the current level of risk is higher than the agreed risk appetite/tolerance and chooses to mitigate consequence and/or likelihood through further action.