Risk Management Policy

Responsible Officer – Director, Eddie Gilmour

Author – Glasgow office

Date effective from May 2023

Date last amended October 2023

Review date September 2025

Contents

Introduction

1 Risk is the uncertainty surrounding events and their outcomes that may have an impact on VIGILO. All our activities carry some risk, arising either from potential threats or the non-realisation of opportunities which may harm, prevent, hinder or interfere with the achievement of our objectives.

2 Risk is inherent in every activity and this policy sets out how VIGILO will manage risks to ensure a balanced approach to opportunity and risk. It explains the approach to risk management; defines risk and how it is assessed, evaluated and escalated in the context of VIGILO's risk appetite; and documents roles and responsibilities for the management of risks.

Risk management

3 Risk management enables organisations to evaluate and respond to risks and opportunities and seeks to manage the impact of uncertainty by increasing the probability of success and reducing the likelihood of failure.

4 Effective risk management involves evaluating the uncertainties and implications within options and managing impacts once choices are made. It provides a process for identifying risks around new, proposed and current business activities, and involves the categorisation and evaluation of each risk and the application of management controls to mitigate the risk. The evaluation is based on a judgement of the likely impact if no further action is taken, combined with an assessment of the likelihood of the risk re-occurring.

5 Risk management should be both an integral part of all organisational activities to support decision-making in achieving objectives and embedded within the culture of the organisation.

Risk identification

6 Like all organisations, VIGILO faces risks, actual and theoretical, that range from the trivial to the existential. This policy is intended to address both the strategic risks which arise from our strategic ambitions and from the potential external threats to VIGILO from the developments in our operating environment, and the operational risks to our objectives and plans to manage and deliver our operational activities.

7 Risk assessment is a qualitative or quantitative evaluation of the nature and magnitude of risk to our objectives and planned activities. The evaluation is based upon known vulnerabilities and threats and considers the likelihood of the threats being realised and their impact on our work.

8 VIGILO Directors and Managers will ensure the strategic risks that may affect delivery of VIGILO's strategy are identified, assessed and included in the strategic risk register which is reviewed by the board of Directors who will continually review the strategic risks to ensure they remain relevant as the operating environment changes and recommend changes, identifying the strategic risks and will also consider risk interdependencies with the client, Police and other key partners.

9 Directors will also ensure that risks in their directorate, which are not strategic in nature, are identified, assessed and incorporated in the operational risk register when they have a potential cross-organisational impact.

10 Directors are required to include a risk assessment in annual reports where there is a substantive new development proposed or substantive change to existing activities.

11 Risk registers are also produced for significant projects, and these will be used to provide mitigations and assurances, for example a large security high risk project, which is not internally facing but is organisation-wide.

Risk assessment

12 Each risk will be assigned an overall assessment depending on its impact and the likelihood of it occurring by applying the approach set out in appendix A. This initial assessment takes account of the mitigating controls in place to manage the risk (for example policies and procedures) and the sources of assurance to assess whether the controls are operating as intended (for example internal audit reviews) and provides a current risk rating. Any further planned actions to reduce the risk score are recorded, with the aim of reaching a target risk rating, using the format in appendix B. The target rating should be informed by the risk appetite (that is set out later in this policy).

13 Risks are scored using a 5x5 matrix giving each risk a score of 1 to 5 for the likelihood of it arising and a score of 1 to 5 for its potential impact on the organisation. In assessing the likelihood of risks arising, a judgement will be made as to whether the possibility of a risk realising is deemed to be rare, unlikely, possible, likely or almost certain. In assessing the impact on the organisation of a risk realising, a judgement will be made as to whether the result is deemed to be very low, low, moderate, high or severe.

14 An overall assessment of each risk is made according to its impact and likelihood of occurrence based on the current controls in place, using the scoring matrix set out in in Appendix A, leading to an overall rating of very low (light green), low (green), medium (yellow), high (amber), very high (red).

Risk treatment

15 Identified risks will be reviewed to determine the action to be taken. This is called the treatment of risks and will be informed by the risk appetite. Options open to treat risks include:

- avoiding the risk, if feasible, by deciding not to start or continue with the activity that gives rise to the risk
- taking or increasing the risk in order to pursue an opportunity or a strategic priority
- retaining the risk by informed decision
- changing the likelihood, where possible
- changing the impact, including planning contingency activities
- sharing the risk with another organisation (eg through a contract or partnership agreement)
- escalating the risk to the client, where appropriate

Alternatively, it may be decided to tolerate the current level of risk, accept the current controls are sufficient and not invest further resources in reducing the risk.

Risk appetite

16 Decisions on risk treatment must be informed by an understanding of the extent to which we are prepared to accept the risks associated with the actions we plan to take. This concept is known as ‘risk appetite’: the extent to which we will tolerate known risks, in return for the benefits expected from a particular action or set of actions.

17 The Board will determine and annually review the risk appetite (set out below) and ensure that planning and decision-making reflects this approach.

18 The concept of risk appetite should be used to inform discussions about how much risk we are willing to bear in the pursuit of our objectives. If properly applied, it results in improved outcomes and use of resources, allowing resources to be prioritised to support the management of risks to achieving outcomes/objectives, whilst maintaining performance and demonstrating value for money.

19 It is often not possible to manage all risks at any point in time to the optimal level, but the ‘risk appetite’ discipline provides a means to guide decisions on when risks should be tolerated.

20 The following section sets out our current risk appetite across the different risk areas using the following definitions:

• Minimalist	Preference for safe options that have a low degree of residual risk
• Cautious	Willing to tolerate a degree of risk where we have identified scope to achieve significant benefit and/or realise an opportunity and the risks can be managed.
• Open	Willing to consider all options and choose one that is most likely to result in successful delivery
• Eager	Keen to be innovative and to choose options that suspend previous held assumptions and accept greater uncertainty

21 It is important to note that risks will not necessarily fit neatly into one of these categories and may intersect across these areas. Therefore, it will be important to use this appetite statement as a guide to inform the approach to managing and accepting risks.

Risk appetite statement

22 Our risk core purpose is to help our client, workers and customers get the best possible service while ensuring safety at all times. We do this by producing guidance for the client and workers by providing rigorous risk assessments, site visits and meeting regularly with clients and staff.

23 Historically VIGILO has had a cautious risk appetite and sought to operate with a low level of risk wherever possible given the impact of our recommendations and need to ensure confidence in our work. However, with the pace of change in the security industry must adopt a more nuanced risk appetite in which we accept, and seek, a wider degree of risk while remaining committed to robust methods, processes, and internal governance.

24 VIGILO has an ambitious transformation strategy to ensure we continue to meet the needs of our key clients. This includes developing new ways of working to ensure our guidance is more relevant, timely and suitable. To achieve these transformation goals, we will maximise opportunities to be more agile, efficient and make the best use of data and new technologies to improve our products and services. We are therefore seeking to accept a greater degree of risk and move towards an open risk appetite across product, process and technology innovation while ensuring the implications of the transformation are managed as set out below. Our risk appetite is premised on the need to ensure compliance with statutory requirements and our obligations.

- **Reputation:** VIGILO is an organisation with a reputation for excellence. Our guidance is scrutinised by our high end corporate clients to provide the highest quality service. We remain committed to retaining this reputation and minimising adverse feedback, but we seek to move towards a cautious appetite for reputational risk in which we recognise the risk of not always taking action or changing the way we work without discussions with all who would be directly affected.

- **Finance:** VIGILO is dedicated to deliver a balanced budget each year. We are required to demonstrate transparency and probity but also ensure the effective use of funding and therefore our appetite for financial risk is cautious, but minimalist to any risk to financial propriety and regularity.

- **Governance:** VIGILO aim to operate with the highest standards of probity and in compliance with all relevant legislation. Our appetite for governance risk is therefore cautious. However, this is premised on the recognition that the approach to governance must be proportionate.

- **Workforce:** Our workforce account for the majority of VIGILO's expenditure and our staff are central to delivering it's objectives. The recruitment market is challenging and there is competition for many of VIGILO's security roles. Therefore, our wider risk appetite for workforce risks is open – reflecting the need to offer specific working arrangements that enhance recruitment and retention, while supporting delivery of the transformation However as a public sector employer, it is vital that VIGILO acts in accordance with the law and good practice and therefore our risk appetite is minimalist to risks to compliance with the statutory employment legislation.

- **IT Security:** A cyber security incident would not have significant implications for VIGILO's activities and reputation. Our appetite for IT security risks is therefore cautious**,** and VIGILO will seek to comply with recognised national standards to mitigate as far as possible any cyber security risks within the available resources. We recognise that it may be necessary to accept a higher level of risk where a particular system/software remains the best available approach to achieving business outcomes.

Assurance

24 The strategic and operational risk registers will outline the assurance on the effectiveness of the controls in place to manage each risk, drawing on the ‘3 lines of defence’ model. An assurance mapping tool is available to help identify any gaps in assurance where action is required to improve the controls.

Oversight

25 The board of Directors have ultimate responsibility for risk management within VIGILO including major decisions affecting VIGILO’s risk profile, appetite or exposure. It will review the strategic risk register annually and periodically dedicate time specifically to identify and consider the nature of emerging risks, sources of uncertainty, threats and trends, and also to reflect on any learning from VIGILO’s response to unforeseen events.

26 Risks may also be removed from the operational risk register if the Directors considers a threat level has decreased significantly or been mitigated sufficiently.

27 The Managing Director, is responsible for ensuring VIGILO has a robust approach to risk management in place and risk is integral to VIGILO’s governance and decision making. They are supported by the Directror and Operations Director, who the lead for risk management, is responsible for leading VIGILO’s overall approach to risk management and ensures that they evaluate the risks identified and apply handling strategies and implement policies to support the process of internal control.

Review

28 This policy will be reviewed every three years or sooner if required (such as publication of new guidance). The risk appetite statement will be reviewed annually.

Appendix A: Quantifying and monitoring risks

Each risk is allocated an **impact** score using the descriptions below ranging from very low with a score of 1 to severe with a score of 5.

Table 1

Category	Score	Examples
Very low	1	• **Financial** - minimal impact on budgets • **People** - minor changes required to working practices • **Objectives / outputs** - no impact on the quality, timeliness or utility of any outputs • **Reputation** - no external challenge or criticism expected • **System impact** – minimal anticipated impact in the Security sector
Low	2	• **Financial** - some impact on one or more budgets, manageable within the budget(s) concerned • **People** - some changes to working practices or minor changes to staff roles • **Objectives / outputs** - minimal impact on the quality, timeliness or utility of any outputs • **Reputation** - some external criticism which is not likely to be material enough to result in reputational damage • **System impact** – potential for some impact in the Security sector
Moderate	3	• **Financial** - material financial consequences for the budget or budgets directly concerned, which can be managed within the affected budget(s) or by the use of underspending in unaffected budgets • **People** - material impact on the employment position of staff, which may need to be managed through formal change processes • **Objectives / outputs** - some impact on the quality, timeliness or utility of any outputs, which can be resolved before publication • **Reputation** - external criticism of the company's judgement, which can be met successfully, and which is unlikely to result in reputational damage • **System impact** – likely to have an impact in the Security sector which will require senior management and/or board discussion
High	4	• **Financial** - material financial consequences, which can only be managed by the use of reserves and/or in year transfers from unaffected budgets.

		• **People** - impact on the employment position of staff, which can only be managed by formal change processes, with risk of redeployment and, exceptionally redundancy • **Objectives / outputs** - significant impact on the quality, timeliness or utility of any outputs, which may require amendment, withdrawal and/or replacement post-publication • **Reputation** - external criticism of the company's judgement, which may result in substantial reputational damage • **System impact** – highly likely to have a negative impact on the security sector which will likely require sustained senior management/board focus and possible discussions with external bodies (SIA etc)
Severe	5	• **Financial** - significant financial consequences which can only be managed by external funding • **People** - protracted unavailability of critical skills/people or high risk of requirement to reduce the headcount through redundancy • **Objectives / outputs** - severe impact on the quality, timeliness or utility of any outputs, which require withdrawal and/or replacement post-publication • **Reputation** - national and international criticism of the Institute leading to sustained adverse media and potential Government intervention • **System impact** – significant negative impact on the security sector which is likely to require SIA and/or wider government action

Similarly, the likelihood of each risk materialising will be assessed on a scale of 1 to 5 as outlined in the table below.

Table 2

Category	**Score**	**Definition**
Rare	1	Highly unlikely to occur in the following 12 months (less than 20% probability)
Unlikely	2	Unlikely to occur in the following 12 months (between 20% but less than 40% probability)
Possible	3	May occur in the following 12 months (between 40% but less than 60% probability)
Likely	4	Likely to occur in the following 12 months (between 60% but less than 80% probability)
Almost certain	5	Highly likely to occur in the following 12 months (greater than 80% probability)

Note: In the case of strategic risks, a timescale of 24 months should be taken into account given the longer-term nature of these risks.

A summative score will be calculated, in each case, by multiplying the impact and likelihood scores, to give a total score. This will lead to an overall rating of the risk. Risks can then be mapped into a risk matrix that has five zones (red, amber, yellow, green and light green).

Table 3

Impact						
	Severe 5	**5** *Low*	**10** *Medium*	**15** *High*	**20** *Very high*	**25** *Very high*
	High 4	**4** *Low*	**8** *Medium*	**12** *High*	**16** *High*	**20** *Very high*
	Moderate 3	**3** *Very Low*	**6** *Low*	**9** *Medium*	**12** *High*	**15** *High*
	Low 2	**2** *Very Low*	**4** *Low*	**6** *Low*	**8** *Medium*	**10** *Medium*
	Very low 1	**1** *Very Low*	**2** *Very Low*	**3** *Very Low*	**4** *Low*	**5** *Low*
		Rare 1	**Unlikely 2**	**Possible 3**	**Likely 4**	**Almost certain 5**
		Likelihood				

When assessing the likelihood and impact of risk, the most credible worst-case scenario should be considered, not the worst-case.

Appendix B: Risk register template (example)

Risk ref	Risk	Lead	Key controls to manage the risk (by lowering the likelihood and/or impact of the risk)	Sources of assurance that the risk is being managed (using 'Three Lines' model)	Current rating			Target rating		
					I	L	S	I	L	S
4	**Organisational transformation** We are unable to …	SR	**<u>Controls currently in place</u>** Leadership development programs for Management, Directors and change leaders **<u>Further actions planned or in progress to lower risk.</u>** Develop 5-year transformation plan leading to integrated behaviors and processes	Key Performance indicators Data from staff surveys Reputation survey results Internal audit of business planning and performance						

Risk: the risk itself, expressed in terms of a cause and an event, and their impact.

Key controls: the actions in place to mitigate the risk, together with any timings (also known as controls). This includes reporting arrangements (e.g. to Board, ARC, ET).

Actions to strengthen mitigation and assurance: the further planned actions to strengthen the controls (to move the current rating to the target rating) and to strengthen the assurance on the controls. This should include dates for completing the actions. The risk owner should ensure that actions are **SMART** (specific, measurable, achievable, relevant, time bound) and that a realistic completion date is assigned to each action.

Sources of assurance: any assurance on the effectiveness of the controls/mitigations, based on the 'three lines' model, with particular emphasis on any sources of external, independent assurance.

Current rating: the score allocated to the impact and likelihood of the risk, and the RAG (Red, Amber, Yellow, Green, Light green) rating allocated to it *after the application of current controls/mitigations.*

Target score: the target score allocated, after the additional proposed mitigating actions, to the impact and likelihood of the risk, and the RAG rating allocated to it.