RISK MANAGEMENT

STRATEGY AND FRAMEWORK

Version	Date	Status	Prepared by	Amendments
1.9	June 2023	Draft	Gill Reid	Review with updates incl. Risk Control Environment, Product Escalation
2.0	Dec 2024		Gill Reid	Annual risk review, group references, strategic pillar, RMC members

Contents

FOREWORD

This document sets out VisitScotland's strategy for addressing risk, and its framework for the identification and appropriate management of risk. Risk management forms an integral part of VisitScotland's internal control environment and corporate governance arrangements, and its success is dependent on its integration within all key activities across the organisation, as well as a proactive approach from all VisitScotland employees who actively contribute to risk management activities in their day-to-day role.

What is a risk?

A risk can be defined as anything that impedes or enhances our ability to meet our current or future objectives as described in our Strategic Plan. It therefore encompasses both **threats** and **opportunities**. These can result from both internal and external factors.

What is risk management?

Risk Management is the term applied to a systematic method of identifying, analysing, evaluating, treating, and monitoring risks associated with our activities in order to help minimise losses and maximise opportunities.

References

VisitScotland's Risk Management Strategy and Framework draws on guidance contained within the Scottish Government's Approach to Risk Management published in March 2011, the Scottish Public Finance Manual, HM Treasury's Orange Book, and the Institute of Risk Management (IRM) publications. It also considers recommendations made by our internal audit contractor concerning process and best practice.

RISK CONTROL ENVIRONMENT

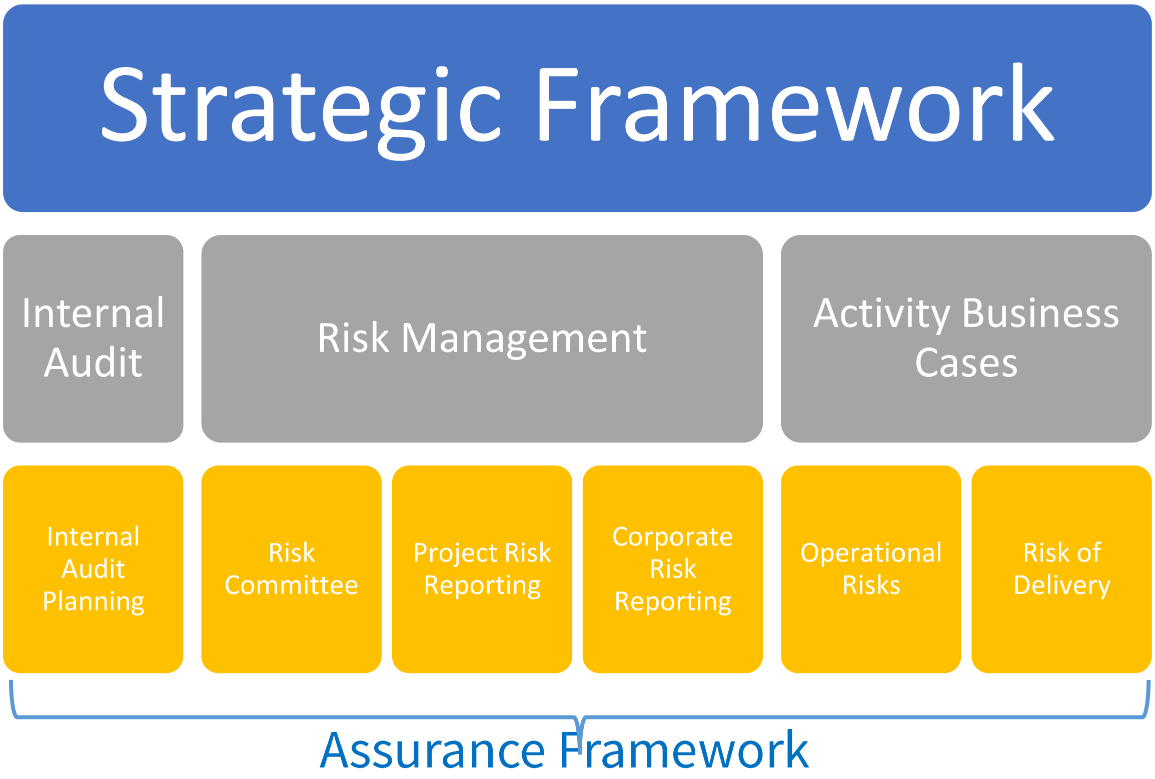
Risk management is embedded into all activities within the organisation and goes beyond the Corporate Risk Register. The risk control environment illustrated in the diagram below shows how management consider risk to be monitored within VisitScotland.

Assurance Framework

An annual review of all key processes which have been mapped to pillars within the Strategic Framework and also to individual risks in the Corporate Risk Register (CRR). This review aims to assess where there may be assurance gaps which need to be addressed. Where there are significant increases/decreases in scoring of the CRR, management re-assess to the levels of assurance and assurance need to ensure they are appropriate.

Activity Business Cases (ABC)

Every activity in the organisation is linked to an ABC. Progress on each ABC is monitored eight times a year, in line with Board meetings and this is then reported in the Financial and Business Performance Report. This reporting captures the risk of unsuccessful delivery at the date of reporting, the year end and in the horizon. In addition to this, each ABC has the functionality to record operational risks for the activity.



VISITSCOTLAND RISK MANAGEMENT STRATEGY

Some level of (negative) risk will always exist and can never be eliminated entirely, so therefore we have a responsibility to manage this risk through an appropriate, and proportionate, risk management strategy in order to support the achievement of our strategic objectives. This is also the case for opportunity risks (positive), as with opportunities which bring benefit/success to the organisation there is still an element of risk involvement that needs managed.

Our risk management strategy will:

- form a component of excellent corporate governance and best management practice through a common approach across VisitScotland.
- provide a sound basis for integrating risk management into decision making.
- integrate risk management into the culture of VisitScotland.
- raise the awareness of staff within the organisation of the need to appropriately manage risk.
- anticipate and respond to changing legislative, economic, environment, and social requirements.
- support the prevention of injury, damage, and losses, and providing a safe working environment.
- ensure that robust mitigating actions are in place to manage identified risks.
- ensure that the objectives of VisitScotland are not adversely affected by significant risks that have not been anticipated.
- ensure that we have reliable contingency arrangements in place to deal with the unexpected which may put service delivery at risk.
- take its lead from the Board with regards to risk appetite.
- ensure the Board is made aware of high-level risks and their potential mitigation when they occur and on an agreed basis thereafter.
- ensure periodic assessment of our attitude to and appetite for risk.
- promote a more innovative, less risk-averse culture in which the taking of appropriate risks in pursuit of opportunities to benefit VisitScotland is encouraged.

The strategy will be implemented by:

- establishing a Risk Management Framework with clear roles, responsibilities, and reporting lines (**see Appendix 3** for VisitScotland’s Risk Management structure).
- appointing a Risk Officer and Risk Management Committee for the organisation with clear terms of reference.
- embedding risk management in to the annual corporate and operational planning process.
- offering guidance and training to managers in their role.
- consulting key staff on circumstances affecting their areas of operation.

- creating risk registers for each significant project and facilitating risk assessment workshops for Project Managers.
- establishing a risk appetite for each of the Strategic Pillars of VisitScotland.
- creating a robust risk register process with regular review by the VisitScotland Executive Leadership Group (ELG), Audit & Risk Committee and the Board.
- establishing monitoring and reporting arrangements through internal review and audit.

Risk management protects and adds value to the organisation and its stakeholders, and the benefits include:

- providing a framework that enables future activity to take place in a consistent and controlled manner.
- improving decision making, planning and prioritisation by comprehensive and structured understanding of business activity, volatility, and project opportunity/threat.
- contributing to more efficient use and allocation of budget resources.
- reducing volatility in the non-essential areas of the business.
- protecting and enhancing assets and reputation.
- protecting, developing, and supporting staff.
- optimising operational efficiency.

Risk Strategy and Framework review process

PROCESS	BY WHO / INPUT	FREQUENCY	OVERSIGHT/APPROVAL
Strategy review	Risk Officer Head of CG&P Dir. Corp Ser *Int. Audit	Min. every 3 years	ELG ARC BOARD (sign-off)
Framework review	Risk Officer Head of CG&P Dir. Corp Ser RMC *Int. Audit	Annually	ELG ARC BOARD (sign-off)

VISITSCOTLAND RISK MANAGEMENT FRAMEWORK

We follow a clearly documented and managed process to ensure that our exposure to risk is acceptable, and that our managers and staff at all levels are equipped to identify, evaluate, manage, and report on risks.

The table below outlines the various roles within the risk management process and their responsibilities:

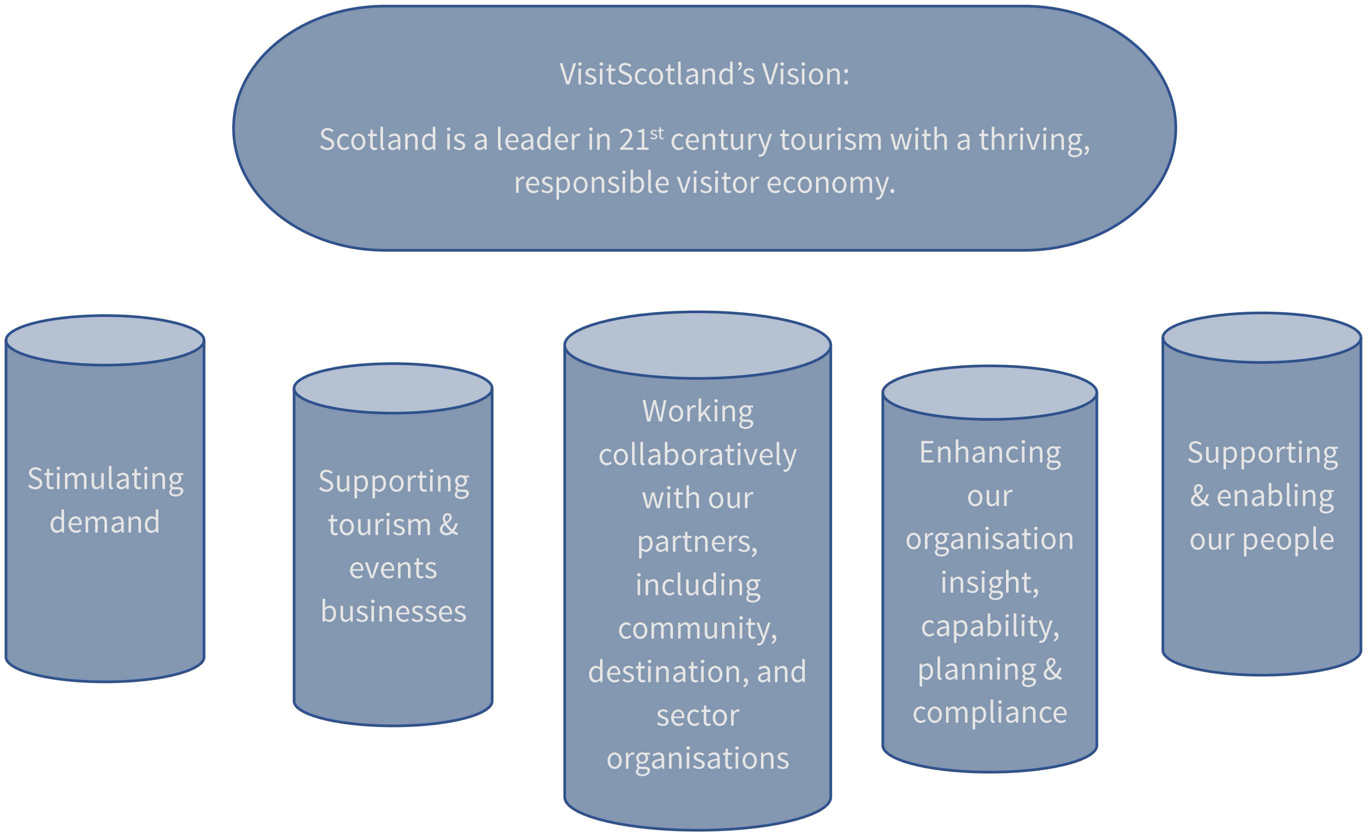
ROLE	RESPONSIBILITY
The Board	Responsible for the strategic direction of VisitScotland, ensuring that it fulfils the aims and objectives set by the Scottish Government. The Board approves risk management arrangements and considers the risk implications of Board decisions. It is informed on risk by the Audit & Risk Committee.
Audit & Risk Committee (ARC)	A sub-committee of the Board which advises the Board on the strategic processes for risk, control, and governance. The processes include the compilation of a corporate risk register and the effectiveness of our management of risk. The Committee monitors effectiveness through reviews, challenge, and internal audit reports on the systems of internal control.
Chief Executive	As Accountable Officer, is responsible for maintaining a sound system of internal control and ensuring a system of risk management is embedded in the organisation. This system is designed to inform decisions on financial and operational planning and to assist in achieving objectives and budgets.
VisitScotland Executive Leadership Group (ELG)	Comprises of the Chief Executive, Directors, and other Senior Management, with overall responsibility for effective risk management and ensuring regular reviews are carried out. Directors are responsible for promoting risk awareness within their operations and ensuring risk management is incorporated at the concept stage of projects. Risk is integrated into the planning and management process and is a standing item for bi-weekly meetings of the ELG.
Director of Corporate Services	Provides leadership and advice on all aspects of corporate governance, audit and risk management to the Board, ARC and ELG, and is VisitScotland's Senior Information Risk Officer (SIRO).

Risk Officer	Oversees and leads on the entire risk management function at VisitScotland. The Risk Officer is responsible for; the Risk Strategy and Framework and ensuring its implementation across the organisation; maintaining the Corporate Risk Register; chairing the Risk Management Committee; leading reviews of risk; drafting a report on risk and assurance for each ARC. The Risk Officer will also consult with colleagues on a regular basis to identify any new or emerging risks, attend project Steering Groups to provide risk management support, and have oversight of all project risk registers.
VisitScotland Risk Management Committee (RMC)	Comprises of senior managers from all areas of the business who meet in advance of each ARC to monitor and review all risk registers (**see Appendix 2** for terms of reference) and oversee risk management arrangements within VisitScotland.
Risk Owners	Those who 'own' and report on a risk for the organisation. These will normally be Directors but can be Heads of Departments, SMEs, or Project Managers.
Mitigating Action Owners	Staff member with responsibility to deliver on specific actions which will mitigate risk.
Project Managers	Responsible for the creation of a project risk register, and management of the risks aligned with their project.
ABC Owners	Prepare risk registers for those ABC (delivery related) risks not covered in the Corporate Register as part of their annual operations plans, and report on progress. They will involve their staff in minimising the effect of risks in their area of operation.
Internal Audit	Review, challenge and report on the adequacy and effectiveness of the system of internal control including audit of risk management and reporting processes.
External Audit	Review and report on the system of financial internal control along with other corporate governance matters including the effectiveness of the risk policy and strategy.

Risk Identification

Risk identification sets out to identify an organisation's exposure to uncertainty. This requires an intimate knowledge of VisitScotland, the market in which we operate, the legal, social, political, and cultural environment in which we exist, as well as a sound understanding of our strategic and operational objectives, including factors critical to our success and the threats and opportunities related to the achievement of these strategies and objectives.

The five Corporate Strategic Pillars outlined in the Corporate Plan for 2024-25 are outlined below and each corporate risk must be assigned to one lead Strategic Pillar:



VisitScotland's Vision:

Scotland is a leader in 21st century tourism with a thriving, responsible visitor economy.

Stimulating demand

Supporting tourism & events businesses

Working collaboratively with our partners, including community, destination, and sector organisations

Enhancing our organisation insight, capability, planning & compliance

Supporting & enabling our people

Risks will be identified through the following channels:

- Risk workshops held annually. Initially with the Heads of Department and Directors group, to refresh the Corporate Risk Register in line with objectives set out in the Corporate Plan. Outputs of which inform the VisitScotland Board annual risk session. At this session the Board will also determine the risk appetite for the coming year.
- Annual planning process includes review of ABC delivery risk by each ABC owner and documentation of the risks associated with the ABC activity, which is reviewed by Head of Governance & Performance and the Risk Officer.
- Risk Management Committee meetings review planning activity and economic and consumer insights to identify any emerging risks, global threats, or trends.

- ELG bi-weekly meetings have risk as a standing item on the agenda and risk is considered when planning or approving new activities or projects, and when reviewing issues arising from business as usual.
- Risk workshops facilitated for significant new projects enable project managers to compile project risk registers which become part of the project management process, and which are reviewed by the Risk Officer and Risk Management Committee ("significant" is determined by the Director of Corporate Services and agreed by the Audit & Risk Committee on a case-by-case basis, taking in to account the scale of the project, resource, time required, and its strategic importance).
- The Policy, Regulation & Legislation Steering Group monitors changing compliance issues, legislation, and accounting practice.
- Internal audit reviews may highlight areas of risk and control weaknesses and recommend mitigating actions.
- Incident and accident reporting, complaints or claims against the organisation may identify risks.

Risk Classification

VisitScotland has classified the type of risk as either *External* or *Internal* with sub-categories according to their nature.

External risks are those over which we have limited/no control but are to do with the nature and purpose of the organisation, its ability to achieve its mission, the environment it works in, its competitors, the stakeholders' needs it seeks to satisfy, its response to opportunities and threats, its vulnerability to political and economic shifts, or the solidity of its reputation and standing.

Internal risks are those which we can control and are to do with the day-to-day operation of the business in areas such as marketing, communications, managing relationships, events, retailing, technology, human resources, facilities, procurement, and finance.

Categories for risks are shown in the table below - they can be external or internal:

CATERGORY	DESCRIPTION
Compliance	Associated with changes in UK or EU legislation, Scottish Government policy or requirements, accounting practice, breaches of regulations etc.
Economic	Relates to global economic factors, UK economy, inflation, foreign exchange rates, industry performance, income levels etc.
Environment	Includes the political environment and factors outside our control which affect tourism in general including terrorism, pandemics, weather, natural disasters.

Reputation	Arising from adverse publicity in the media, trade criticism, brand damage, crisis management etc concerning VisitScotland and/or the tourism industry.
Finance	Associated with funding levels, reduction in income, budgetary control, financial planning, cost effectiveness, financial controls, fraud etc.
Governance & Strategy	Includes industry engagement, stakeholder management, partnerships, branding, marketing campaigns, competition, strategic decision making.
Process	Associated with operational matters including contractual arrangements, organisation structure, human resources, business continuity, health & safety.
Technology	Relates to IT infrastructure, capital investment, pace of technological change, systems, websites, data security, disaster recovery, third party hosting etc

Nature of risk types are shown in the table below:

NATURE	DESCRIPTION
Strategic	Long-term or opportunity risk concerned with where the organisation wants to go and how it plans to get there, and impacts on the achievement of the strategic aims of the organisation.
Operational	A risk that could occur from inadequate or failed internal processes, people or systems, and capable of impacting the operation of the organisation.
Project	Significant projects will have risk registers which will manage those risks that could present doubt on our ability to deliver a project on time, within budget and to scope.
Horizon	External risk in which it's likelihood of occurring is out-with the control of the organisation.

Risk Management Process

Successful risk management requires the identification and recording of key risks and an assessment of the level of the risk in terms of **likelihood** of occurrence and scale of **impact** on the organisation, including consideration of the current methods of managing that risk. From this process actions can be agreed to mitigate these risks, with ownership assigned to appropriate individuals. Regular monitoring then needs to take place to ensure that actions are implemented, risks reduced, and any new risks identified.

Our approach to the management of risk can be summed up as follows:

1. Identify, evaluate, and prioritise the key risks facing VisitScotland.
2. Complete a Risk Register categorising and listing all the risks identified.
3. Assess the impact and likelihood of the risk occurring.
4. Assign each risk to an individual and identify existing controls and responses which address and minimise the risk - risks can be allocated at Head of Department, Project Manager, or Director level, or to a SME.
5. Where there are insufficient or ineffective controls or responses, formulate new controls and an action plan to address the risk.
6. Regularly review and re-score risks and report on responses to risks at the Leadership Group, RMC, ARC and Board.
7. Embed risk assessment into the working practices and planning processes at VisitScotland so that staff become focused on meeting objectives by managing significant risks.

Risk Registers

VisitScotland has a **Corporate Risk Register** (CRR) which documents the significant strategic, operational, horizon and project risks identified by the Board and Management.

The CRR (**see Appendix 1** for template) includes the current and planned mitigating actions and controls for each identified risk, the person responsible for the action/activity, and an assessment of the likelihood and impact of the risk occurring. All risks must be reported in this manner, including, ‘major’ projects. Additionally, major projects reported on via the CRR must also maintain a project-specific risk register which details all the risks faced by the project and the mitigation in place to manage the risk.

Project Risk Registers

All major new initiatives and significant projects (those held in the CRR or not) will undergo a risk assessment process which will generate a project-specific risk register to be owned and maintained by the Project Manager and reviewed by the Risk Officer and the project’s Steering Group (**see Appendix 6** for Project Risk Register template). This forms part of the VisitScotland’s standard project management methodology as overseen by the Portfolio Office.

The Risk Officer will provide advice and guidance on the effective management of risk to Project Managers, which should include a brain-storming session of risks with the project team in order to identify all risks associated with the project. The initial project risk register (CRR held projects only) is also reported to the Audit & Risk Committee by the Project Manager with any updates as considered appropriate.

Project Manager’s should review and score the risks within their project risk register on a regular basis, tracking overall ‘project’ and ‘immediate’’ progress. All major projects will provide both overall *project* (long-term project deliverability) and overall *immediate* (short-term issue management) progress updates and scores for the quarterly Risk Report (CRR held projects only).

Assessing Impact and Likelihood of a risk

See Appendix 5 for Risk Matrix.

The maximum score for a risk is 25 (Impact 5 x Likelihood 5). Guidance on risk scoring levels for impact and likelihood is given in the table on Risk Scoring below.

Initial scores are recorded for each risk:

Untreated / Gross - before taking in to account any mitigating action or controls in place.

Target / Net / Residual - after taking any ongoing or planned action and controls into consideration.

Risk Scoring Guidance

LEVEL OF IMPACT	1 – VERY LOW / NEGLIGIBLE	2 – LOW / MINOR	3 – MEDIUM / MODERATE	4 – HIGH / MAJOR	5 – VERY HIGH / EXTREME
Strategic	Little impact on the organisational strategy.	May have an impact on achieving organisational strategy but this could be resolved.	Would impact on the organisational strategic objectives and would require management discussion.	Would require a significant shift from organisational strategy objectives that would require Leadership/ARC input.	Would require a fundamental change in organisational strategic objectives.
Operational	Has no impact on the day-to-day operation of the organisation. Less than 1 month's delay in delivery of the project/activity.	Low level processes would need to be revised but the matter could be resolved. Delay 1-3 months in the delivery of project/activity.	A significant amount of work would be required by a team to repair operational systems. Delay 3-6 months in delivery of project/activity.	A significant amount of work would need to be done at all levels to resolve the matter. Delay 6-12 months on delivery of the project/activity.	Fundamental organisational changes would need to be implemented. Delay of 1 year+ in delivery of project/activity.
Financial	If the risk materialised the cost to the organisation would be no more than £10k*	If the risk materialised the cost to the organisation would be between £10k-£100k*	If the risk materialised the cost to the organisation would be between £100k-£500k*	If the risk materialised the cost to the organisation would be between £0.5m-£1m*	If the risk materialised the cost to the organisation would be greater than £1m>*
Reputational	Has no negative impact on the organisation's reputation/no media interest.	Minor damages in a limited area. May have localised, low level negative impact on the organisation's reputation/generates low level of complaints.	Minor damages but widespread. Significant localised low-level negative impact on the organisation's reputation/generates limited complaints.	Significant negative impact on the organisation's reputation. Could impact on org's ability to influence public / Industry /Stakeholder's /Government. Generates significant number of complaints.	Significant and irreparable damage to reputation. Sustained negative publicity resulting in loss of public/Industry/Stakeholder confidence in organisation.

Compliance	No impact on the organisation’s governance structures.	May breach low level governance regulations but can be rectified.	Breaches governance regulations and would require significant work to rectify.	Significant breach of governance regulation requiring immediate notification of regulatory bodies.	Serious breach of governance regulations/legislation that would lead to the status of the organisation being reviewed.

LIKELIHOOD	**1 - RARE**	**2 - UNLIKELY**	**3 - POSSIBLE**	**4 - LIKELY**	**5 – ALMOST CERTAIN**
	Not occurring very often; unusual	Not likely to happen; improbable	Able to be achieved; can be done	This will probably happen; to be expected	Nearly definite; no likely other outcome

Risk Appetite

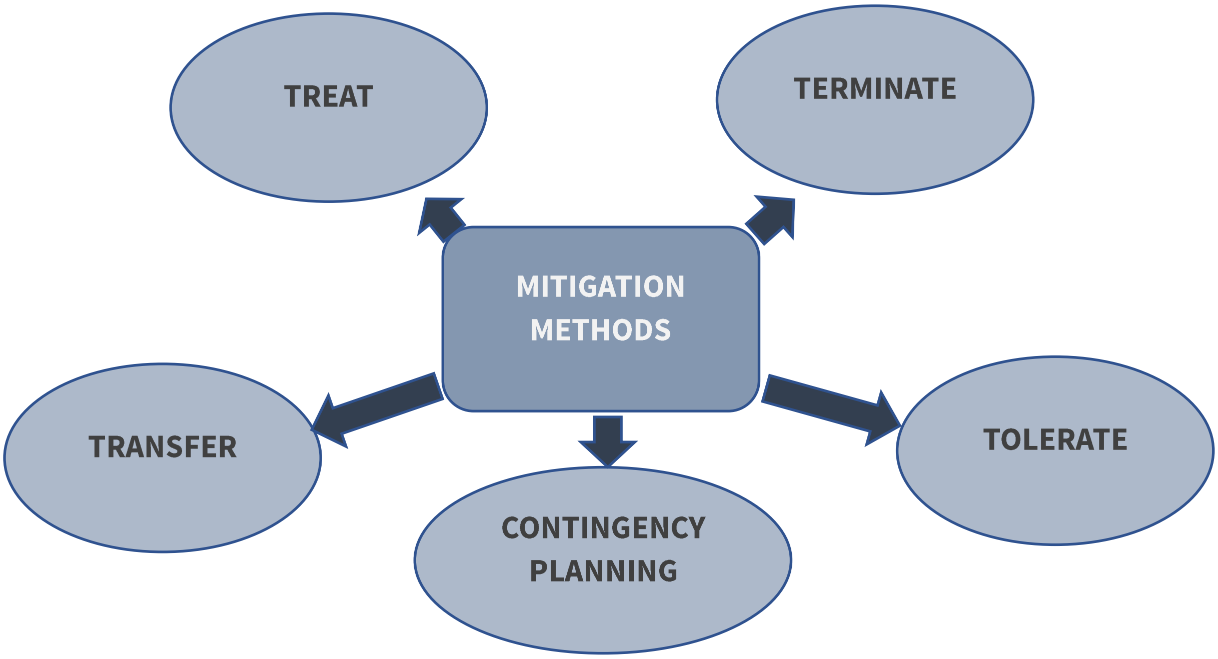
The aim of effective risk management is not to remove all risk but to recognise that some level of risk will always exist. Risk appetite can be defined as the amount and type of risk that the organisation is willing to take in order to achieve its strategic objectives. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance. Risk appetite is deemed to be the acceptable level of risk before any mitigation.

Note that some risk is un-avoidable, and it is not within the ability of VisitScotland to completely manage it to a tolerable level - for example many organisations must accept that there are global economic factors which they cannot control. In these cases, VisitScotland will make *contingency plans*.

The risk appetite of the organisation is determined by the Board at Strategic Pillar level, with an appetite applied to risk in its inherent (gross) state. The Board also determines the risk appetite for the activities carried out within each Strategic Pillar, depending on their nature (**see Appendix 4** for Risk Appetite).

Options for Managing Risks (Mitigation)

Risk management is not simply about identifying risks and then avoiding them. It is about managing those risks in the most efficient and effective manner. External and internal risks are identified, objectively assessed, scored using quantitative methods and, where this is the appropriate response, actively managed. The most common forms of dealing with or responding to risk are:



TREAT - action is taken to reduce the likelihood or impact of the risk. The key is that any action must be cost effective against the size and impact of the risk.

TERMINATE - do something differently thereby removing the risk completely. Care should be taken that any alternative approach does not create bigger risks.

TRANSFER - the risk's financial impact or the responsibility for managing it is given to someone other than VisitScotland. This can usually be achieved by contracting out the activity or through insurance or penalty clauses.

TOLERATE - this response to a risk is really the response of last resort. Tolerating the risk involves accepting a risk above our acceptable level without reducing it, probably because nothing can be done to reduce it at a reasonable cost.

CONTINGENCY PLAN - the impact or likelihood of the risk cannot be reduced to an acceptable level (or even when it can) then contingency plans should be devised to ensure business continuity and recovery after events that cannot be controlled. Contingency plans should as a minimum be considered for all risks with expected high impact or high likelihood. Contingency plans should always be tested.

Risk Proximity

Risk proximity can be defined as, how close we are, in terms of time, to a risk potentially occurring. Assessing and applying the proximity of a risk allows for risk prioritisation. We need to assess when the risk is likely to occur so that we can respond to it appropriately. Risk proximity is used to ensure that focus on risks is balanced, with a greater focus on those risks that are likely to occur immediately to short term.

The table below outlines fixed proximity categories that should be applied to risks within a risk register.

PROXIMITY	
Immediate	unknown – could occur at any time
Imminent	predicted to occur within the next 3 months
Short-term	predicted to occur within the next 3-12 months
Medium-term	predicted to occur within the next 1-3 years or is aligned to our Strategic Framework
Long-term	predicted to occur within the next 3+ years

It is important that ongoing monitoring of a risks' proximity is carried out when undertaking review of the risk register, in the eventuality of a change to the risk horizon.

Risk Reporting

The Corporate Risk Register is reviewed by Management and reported on to the Audit & Risk Committee on a quarterly basis, which includes exception reporting on the current amber and red risks.

Risk Level	Risk Level Description
Extreme	**Rating**: Unacceptable level of risk exposure that requires immediate mitigating action. **Reporting**: To Chief Executive, Audit & Risk Committee, and the Board.
Very High	**Rating**: Unacceptable level of risk exposure that requires immediate mitigating action. **Reporting**: To Chief Executive, Audit & Risk Committee, and the Board.
High	**Rating**: Unacceptable level of risk which requires controls to be put in place to reduce exposure. **Reporting**: To Chief Executive/Audit & Risk Committee for upward reporting to the Board.

Medium	**Rating**: Acceptable level of risk exposure, subject to regular active monitoring. **Reporting**: At Risk Management Committee/ Leadership Group level.
Low	**Rating**: Acceptable level of risk, subject to regular passive monitoring. **Reporting**: To Risk Management Committee. Consideration should be given as to whether risks recorded as low are still extant.

At each meeting of the VisitScotland Risk Management Committee a review will be undertaken of the Corporate Risk Register to ensure that it accurately reflects VisitScotland's current risk profile and that the mitigation in place remains appropriate. The report on risk made to the VisitScotland ELG and the ARC should consider:

- Progress made with mitigating actions to address each risk.
- The Corporate Plan objectives, performance targets and departmental or area risks identified.
- Any other new or changed risks or changed likelihood or impact of risks.
- Assurance 'need' vs current assurance levels, and any remedial action required.
- Insights and scenario planning activity including creation of any contingency plans.
- Any changes in responsible officers.
- Reports from auditors, if appropriate.

The reviews will include cooperation with Directors, Senior Managers, and SMEs, and will highlight any necessary training and awareness on risk management arising from the review.

The Risk Officer prepares the report in league table format clearly showing the ranking of risks based on scoring, and with a summary of mitigating actions for all high-level risks. Risks with significant score increases or decreases are highlighted together with explanations.

A summarised version of the red and amber risks is included in the Measurement Report issued to the Board, along with any other updates on risk as deemed appropriate by Management.

Product Escalation and Reporting

When a project involving a key digital system has been delivered the project is closed and the system moves into 'product' status, in that it is fully operational and part of BAU.

Any significant increases in the level of risk for a product will, in the first instance, be escalated to the VisitScotland Leadership Group.

Reporting on product risk status will form part of the quarterly risk reporting to RMC, VisitScotland ELG, ARC, and Board (where appropriate).

Risk Status

Every risk within the Corporate Risk Register has an assigned status at any given time, with this influencing the reporting requirements for the risk in the quarterly Risk Report.

The table below outlines the status that can be assigned to a risk:

RISK STATUS	
Active	Open risk currently within VisitScotland risk profile. Owner updates and ARC reporting required
Closed / Inactive	Risk no longer within VisitScotland risk profile. No Owner updates or ARC reporting required
Deactivated	Risk no longer within VisitScotland risk profile (at present) but may re-emerge in future and therefore should not be 'closed'. Owner updates not required, but oversight via quarterly Risk Report

Risk in the Planning Process

To be effective, risk management needs to be embedded within the planning process. This will assist Directors, Senior Management, and the Risk Officer in identifying new key risks or significant changes to existing ones. Each ABC will include a key risk register for the project/activity. The risk updates will be reviewed by the Risk Officer on an ongoing basis.

The ABC/Project Owner will own, promote, and review the risk management process for their ABC and encourage and support their teams in understanding how their actions can help to minimise the key risks to their area/department's objectives and activities.

The key risks will be reviewed regularly when reporting on progress against objectives, and any significant new risks or changes to existing risks will be brought to the attention of the appropriate Director or VisitScotland ELG.

Assurance Framework

VisitScotland's *Assurance Framework* forms as integral part of our governance processes. Over 180 assurance activities (our 'Audit Universe') are mapped across key business areas under each Strategic Pillar and aligned to risks within the Corporate Risk Register. An initial exercise is carried out wherein each assurance activity is assessed by the Risk Officer, Head of CG&P and SME, to identify the 1st, 2nd and 3rd Lines of Defence currently in place, and which will highlight any gaps in assurance. These gaps are shared and evaluated with our Internal Audit partner and can influence the VisitScotland Internal Audit Plan.

There are three **Lines of Defence:**

First Line of Defence – Management control / review, e.g., Policies, Workplace Assessments, ABCs, Security/Pen tests, Staff Survey, Campaign Evaluations

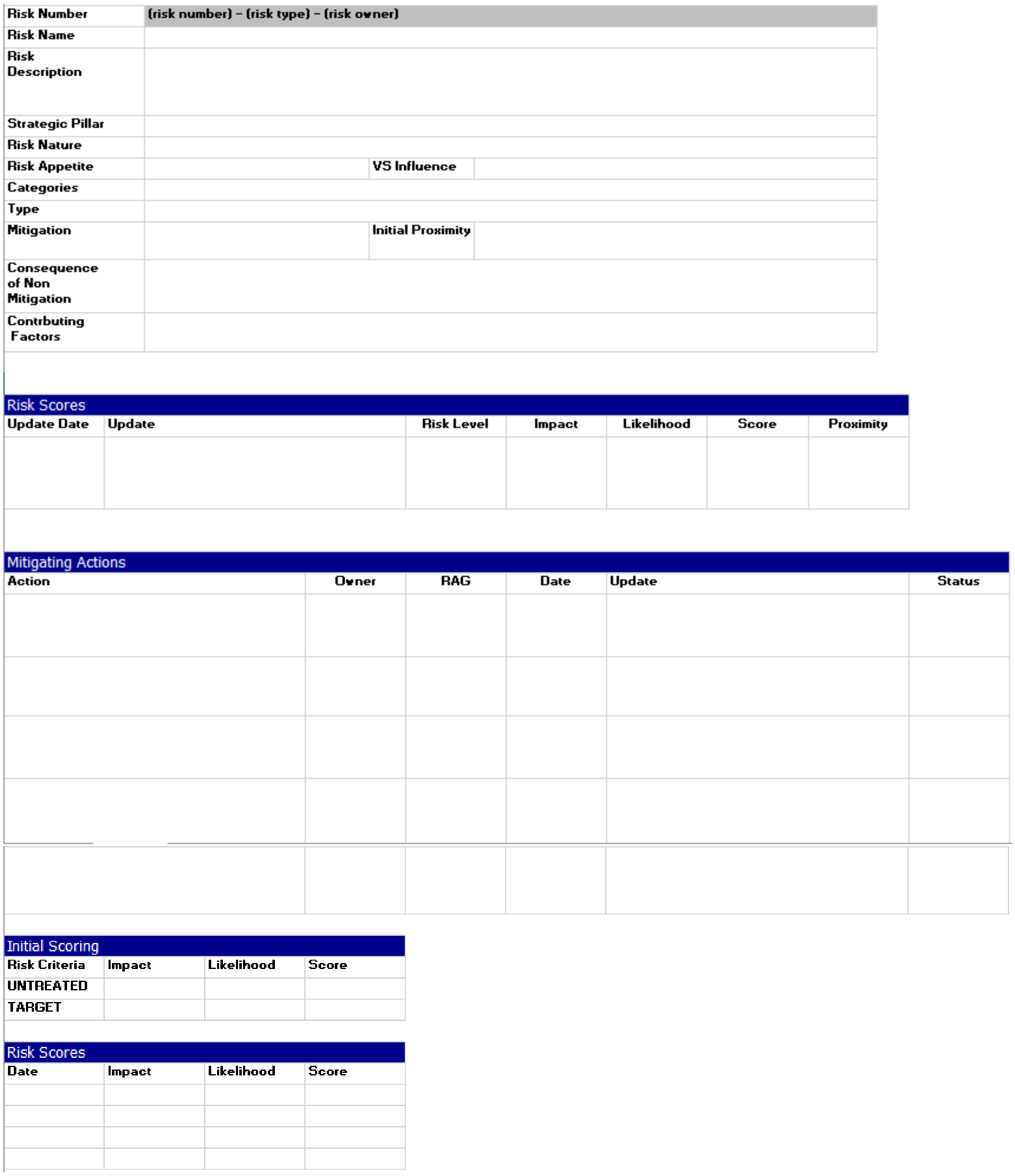
Second Line of Defence – Internal independent oversight, e.g., DGSG, RMC, PDB, ARC/Board, Funding panels

Third Line of Defence – External independent oversight, e.g., Internal / External Audit, SG reporting, Gateway reviews

Every quarter, as part of risk reporting, the Risk Officer carries out assessment of each corporate risk to determine its assurance need vs current assurance level, which highlights any further remedial action required. This detail is included within the quarterly Risk Report that is presented to the VisitScotland RMC, ELG, ARC, and the Board.

A full review of all assurance activities (Audit Universe) and their assurance need is undertaken on an annual basis, to ensure that the VisitScotland Assurance Framework remains up-to-date and maintains an appropriate level of assurance (control) for all key business processes.

APPENDIX 1 – Corporate Risk Register Template



Risk Number	(risk number) – (risk type) – (risk owner)		
Risk Name			
Risk Description			
Strategic Pillar			
Risk Nature			
Risk Appetite		VS Influence	
Categories			
Type			
Mitigation		Initial Proximity	
Consequence of Non Mitigation			
Contrbuting Factors			

Risk Scores

Update Date	Update	Risk Level	Impact	Likelihood	Score	Proximity

Mitigating Actions

Action	Owner	RAG	Date	Update	Status

Initial Scoring

Risk Criteria	Impact	Likelihood	Score
UNTREATED			
TARGET			

Risk Scores

Date	Impact	Likelihood	Score

APPENDIX 2 – Risk Management Committee Terms of Reference

Purpose

The purpose of the Risk Management Committee is to oversee risk management arrangements within VisitScotland, and to support and advise the Risk Officer, Leadership Group, Audit & Risk Committee, and the Board on the implementation and monitoring of the VisitScotland Risk Management Strategy and Framework.

The Committee will meet in advance of each Audit & Risk Committee meeting. Any significant issues or concerns arising from the meetings will be submitted to the Leadership Group and to the next meeting of the Audit & Risk Committee. The work of the Committee will contribute to giving the appropriate assurance to Management, ARC, and the Board that all aspects of risk within VisitScotland are adequately managed.

Key Role and Responsibilities

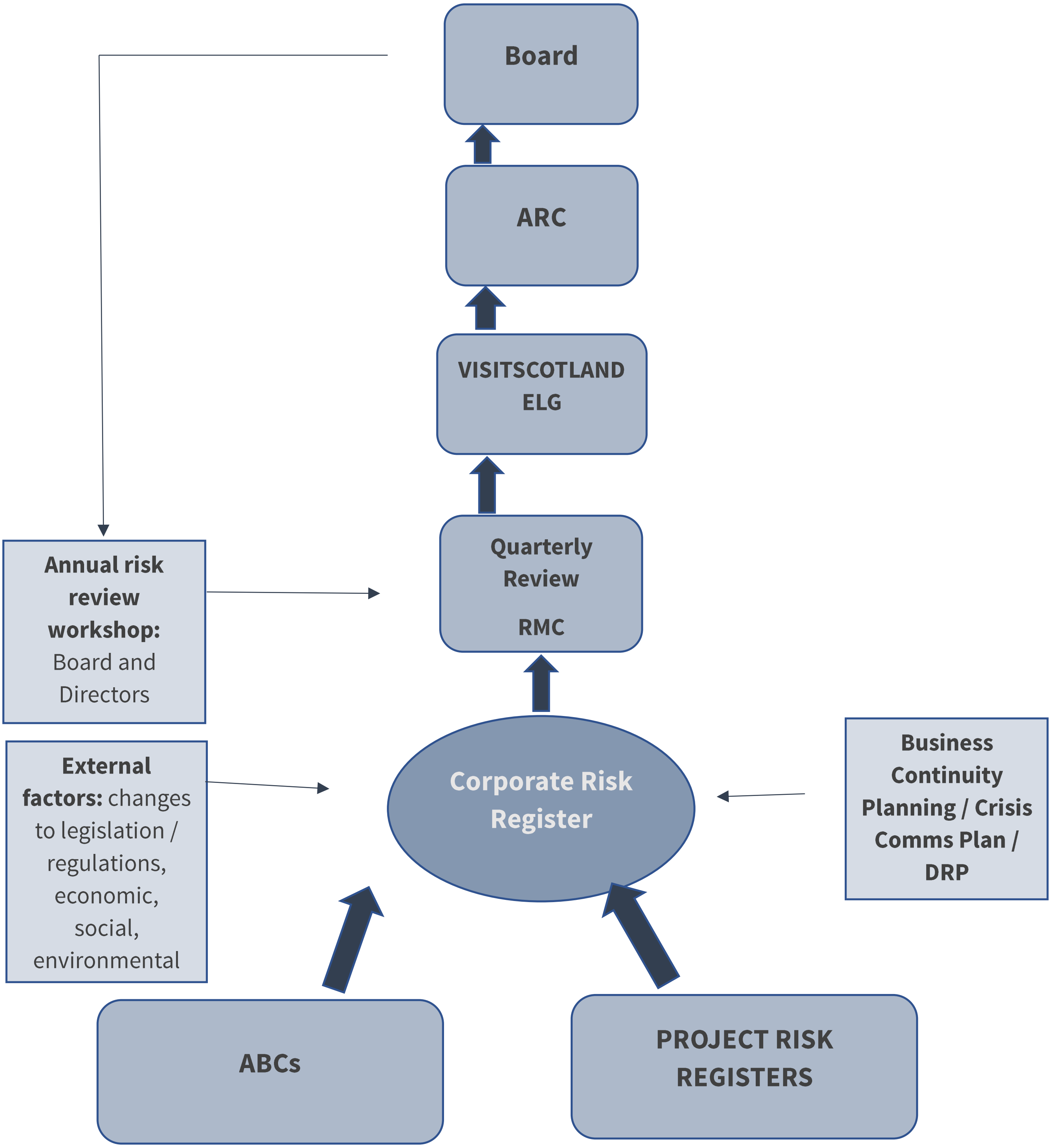
- Assist the Risk Officer in promoting risk management throughout VisitScotland by encouraging managers to address the key risks which threaten the achievement of VisitScotland's objectives.
- Ensure that risk management is included within the annual planning process and considered within departmental plans and all major project planning, and review the risks highlighted in those plans.
- Review strategic, economic, and other research activity to identify any new, emerging or changing external risks which might affect VisitScotland's objectives.
- Oversee and contribute to the ongoing review of the risk registers each year presented to the VisitScotland Leadership Group, the Audit & Risk Committee, and the Board.
- Assess the adequacy of and monitor the progress of the mitigating actions identified in the risk registers, departmental plans and major projects.
- Ensure that all significant risk management concerns, including new, emerging, or changing risks, are properly considered, prioritised and communicated to the Leadership Group.
- Ensure that business continuity issues are reflected in the risk register and seek confirmation that business continuity arrangements and plans are maintained and kept up to date.
- Assist the Risk Officer in identifying the risk management training needs within the organisation.

Composition

Chair: Gill Reid, Risk and Compliance Officer – Corporate Governance & Performance
Members:
Ken Neilson, Director of Corporate Services and SIRO
Michelle Lavery, Head of Corporate Governance & Performance
Martin Bowie, Senior Portfolio, Risk and Performance Manager - CG&P
Ken Massie, Head of Destination Development – Industry and Events
Marie Christie, Head of Development, Events Industry – Industry and Events
Leanne Mallon, Head of Performance Marketing – Marketing & Digital
Richard Lamont, Reward, Benefits & MI Manager – HR
Carolyn Churchill, Head of Corporate Communications

Edward Mitchell, Cyber Security Specialist - IT
Raymond MacIntyre, Insight Economist – Insights
Allan Henderson, Head of Digital Delivery – Marketing & Digital
Rachel Rennie, Senior Programme Manager – Marketing & Digital
Andy Bruce, Portfolio Manager – Corporate Governance & Performance
Jill Brownell, Governance Manager – Corporate Governance & Performance

APPENDIX 3 – Risk Management Structure



Board

ARC

VISITSCOTLAND ELG

Quarterly Review

RMC

Annual risk review workshop: Board and Directors

External factors: changes to legislation / regulations, economic, social, environmental

Corporate Risk Register

Business Continuity Planning / Crisis Comms Plan / DRP

ABCs

PROJECT RISK REGISTERS

APPENDIX 4 – Risk Appetite

Risk appetite is aligned to risk at its inherent (gross) level before any mitigation has been applied.

Risk Appetite Definitions	
Hungry	Eager to be innovative and pursue opportunities offering potentially high rewards despite greater inherent risk.
Open	Willing to consider all opportunities that offer the potential for significant reward but may also present significant inherent risk.
Cautious	Preference for safe delivery options that have a moderate degree of inherent risk and may only have limited potential for reward.
Minimalist	Preference for ultra-safe business delivery options that have a low degree of inherent risk and only have a potential for minimal reward.

The current risk appetite for each of the Strategic Pillars is shown in the table below:

Strategic Pillar	Appetite
Stimulating global demand	Hungry
Supporting Scotland’s tourism & events businesses	Hungry / Open
Working collaboratively with community, sector & destination organisations towards a responsible recovery	Open
Enhancing our organisation insight, capability, planning & compliance	Open
Supporting & enabling our people	Open

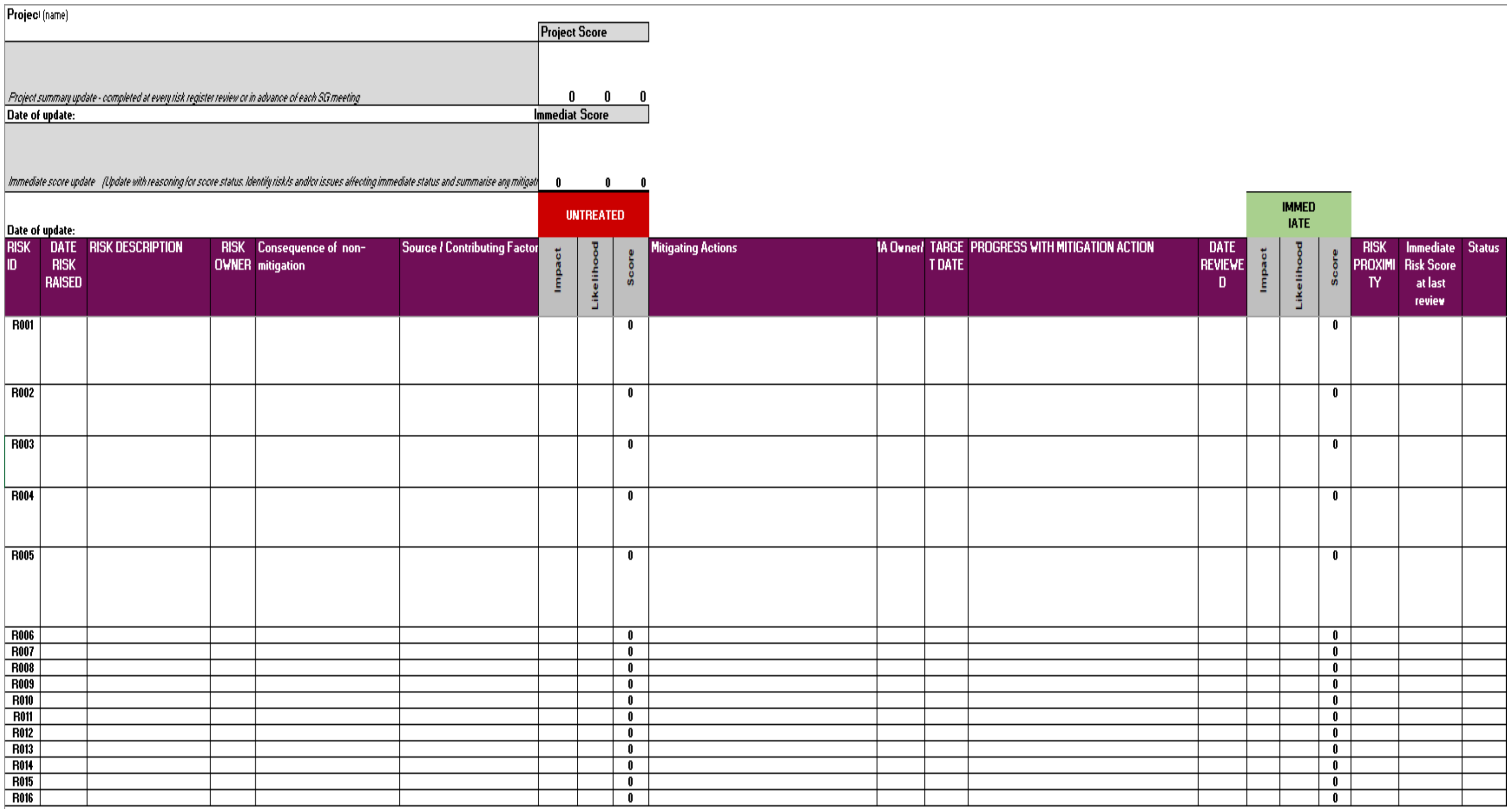
The current risk appetite for each of our activities descriptor is shown in the table below:

Nature of activity	Appetite
Mandatory	Hungry
Transformational	Hungry
Strategic	Hungry
Compliance	Cautious
Business as usual (BAU)	Open

APPENDIX 5 – Risk Matrix

Likelihood	Multiplier					
Almost certain	5	5 Medium	10 High	15 High	20 V High	25 Extreme
Likely	4	4 Medium	8 Medium	12 High	16 High	20 V High
Possible	3	3 Low	6 Medium	9 Medium	12 High	15 High
Unlikely	2	2 Low	4 Low	6 Medium	8 Medium	10 High
Rare	1	1 Low	2 Low	3 Medium	4 Medium	5 High
	Multiplier	1	2	3	4	5
	Impact	Negligible	Minor	Moderate	Major	Extreme

APPENDIX 6 Project Risk Register Template



Project (name)						Project Score														
Project summary update - completed at every risk register review or in advance of each SG meeting						0	0	0												
Date of update:						Immediat Score														
Immediate score update (Update with reasoning for score status. Identify risk/s and/or issues affecting immediate status and summarise any mitigati						0	0	0												
Date of update:						UNTREATED								IMMED IATE						
RISK ID	DATE RISK RAISED	RISK DESCRIPTION	RISK OWNER	Consequence of non-mitigation	Source / Contributing Factor	Impact	Likelihood	Score	Mitigating Actions	A Owner/	TARGET DATE	PROGRESS WITH MITIGATION ACTION	DATE REVIEWED	Impact	Likelihood	Score	RISK PROXIMITY	Immediate Risk Score at last review	Status
R001								0								0			
R002								0								0			
R003								0								0			
R004								0								0			
R005								0								0			
R006								0								0			
R007								0								0			
R008								0								0			
R009								0								0			
R010								0								0			
R011								0								0			
R012								0								0			
R013								0								0			
R014								0								0			
R015								0								0			
R016								0								0			

APPENDIX 7 – List of Related Documents

This list covers the main documents which impact on or relate to risk management. It is not an exhaustive list.

VisitScotland 3-year Corporate Plan
Strategic Framework
Activity Business Cases (ABCs)
Business Continuity Plan
Crisis Communications Manual
Fraud Policy and Fraud Response Plan
Whistleblowing Policy
Corporate Governance Framework
Health & Safety Policy
Freedom of Information Publication Scheme
Information Systems Acceptable Use Policy
Data Security and Information Risk Policy
Policy for Identification and Treatment of Confidential Information
Statement of Internal Control in the Annual Accounts
Certificate of Assurance
Corporate Risk Register
Project risk registers
Project Management Handbook
Internal audit reports
External audit reports

APPENDIX 8 – Risk Management Glossary

ABC: 'Activity Business Case'**.** Document which captures, and records information needed to correctly define and plan a project e.g., project goals, scope, business case, costs, milestones, risks**.**

Assurance Framework: Part of VisitScotland governance processes. Assurance activities and their assurance 'need' mapped across key areas (under Strategic Pillars) and to risks within Corporate Risk Register.

Contingency Planning: The process of identifying and planning appropriate responses to be taken when, and if, a risk occurs.

Corporate Governance: The Audit Commission defines Corporate Governance as *"the framework of accountability to users, stakeholders and the wider community, within which organisations take decisions and lead and control their functions, to achieve their objectives."*

Corporate Risk Register: A formal listing of identified risks that could impact on the delivery of the organisations strategy, together with the results of the risk analysis and risk evaluation procedure, as well as details of any risk treatments.

Crisis Communications Manual: Document written to provide a crisis "checklist" to ensure that VisitScotland staff are as prepared as they can be, can respond as quickly as possible to a critical situation, and can limit further damage.

Exposure: The susceptibility to risk or loss.

Impact: Effect or consequences of a risk should it occur.

Incident: An event or circumstance which could have or did lead to unintended and/or unnecessary harm to a person, and/or a complaint, loss, or damage.

Initial/Untreated Score: The "pure" risk score before considering mitigating actions or controls already in place.

Likelihood: A qualitative description of a probability or frequency of the risk event occurring.

Mitigating Action: Any action that seeks to reduce the likelihood or impact of a risk event to an acceptable level.

Mitigating Action Owner: A member of staff who has responsibility to deliver on specific actions which will mitigate risk.

Objective Something worked toward or striven for, a goal.

Opportunity: An uncertain event with a positive probable impact.

Project Manager: The person with overall responsibility for the planning and execution of a project, and for the creation of the risk register for their project.

Residual risk: The level of risk remaining after managing it through treatment and/or control measures.

Risk: The chance of something happening that will have an impact on business objectives. It is defined as the combination of the probability (likelihood) of an event and its consequences (impact). Risks can bring both negative and positive impacts.

Risk Analysis: The use of information to work out how often something might occur and the size of the impact.

Risk Appetite: The level of exposure to risk which is considered tolerable and above which further action must be taken.

Risk Assessment: The identification and measurement of risk, and the process of communicating about these risks.

Risk Categories: There are, in practice, different types of risk, external and internal, which can be sub-categorised as Compliance, Economic, Environment, Reputation, Finance, Governance and Strategy, Process, Technology.

Risk Identification: The process by which risk events, which could affect the organisation's objectives, are identified, described, and recorded.

Risk Management: Risk Management is the term applied to a systematic method of identifying, analysing, evaluating, treating, and monitoring risks associated with activities in order to help minimise losses and maximise opportunities.

Risk Matrix: A model that visually displays the relationship between the likelihood and impact of specific risks. Visually it is a 5x5 box that plots likelihood and impact scores from low to high.

Risk Owner: A nominated person who is responsible for a risk by ensuring the existence and effectiveness of mitigating actions.

Risk Prioritisation: The process of ranking risks into a logical order by establishing how significant they are in terms of likelihood and impact.

Risk Proximity: A measure of how close we are, in terms of time, to a risk potentially occurring.

Risk Strategy: The overall organisational approach to risk management.

Risk Treatment: Selection and implementation of appropriate options for dealing with a risk.

Target Score: The remaining risk score after considering mitigating actions and controls in place.

Terminate: An informed decision not to become involved in a risk situation. (i.e., to choose another path, which does not encounter that risk)

Threat: A combination of risk, the consequences of that risk, and the likelihood that the negative event will take place.

Tolerate: An informed decision to accept the likelihood and the consequences of a risk, rather than trying to mitigate it.

Transfer: An informed decision to transfer the risk to another party, who will accept the risk through contracting out or insuring against it.

Treat: An informed decision to take additional action to further minimise the likelihood or impact of an identified risk.