Revenue Scotland

Risk Management Framework

Revenue Scotland
Teachd-a-steach Alba

Document Control

Title	Revenue Scotland Risk Management Framework
Prepared by	Gary Sharp
Approved internally by	Chief Executive and Senior Leadership Team
Date of approval	
Version number	2.0
Review frequency	Every 6 months
Next review date	June 2019

Status Control

Version	Date	Status	Prepared by	Reason for amendment
0.1	15/07/2015	Draft	Denise McCann	Creation of Document
0.2	30/01/2017	Published	Brian Rigby	Amendments
0.3	26/06/2017	Published	Brian Rigby	Amendments
1.0	19/04/2018	Published	Grant Neilson	Control sheet added
1.1	16/10/2018	Draft	Gary Sharp	Review of risk management
2.0	12/12/2018	Approved	Gary Sharp	Publish approved version

Contents

1. Introduction

This document sets out Revenue Scotland's approach to risk management and outlines the key objectives, strategies and responsibilities for the management of risk across the organisation. It applies to all Revenue Scotland staff and should be applied consistently across the organisation. It will be supported by training to ensure that staff are risk 'aware'.

2. Policy statement

2.1 Revenue Scotland is committed to ensuring that the management of risk underpins all business activities of the organisation and that thorough risk management procedures are in place throughout the organisation.

2.2 The application of this Framework will enable Revenue Scotland to obtain, maintain and respond to a changing risk profile.

2.3 Revenue Scotland has a responsibility to manage risks (both positive and negative) and to support a systematic approach to risk management including the promotion of a risk aware culture. This requires risks to be regularly identified, reviewed and updated.

2.4 The application of risk management practices should not and will not eliminate all risk exposure. Moreover, through the application of the risk management approach identified in this Framework we aim to achieve a better understanding of the risks faced by Revenue Scotland and their implications for the business, thus informing decision-making.

2.5 Revenue Scotland recognises that risk, as well as posing a threat, also represents opportunities for developing innovative ways of working. Innovation and best practice should be shared across Revenue Scotland.

2.6 The identification and management of risks affecting Revenue Scotland's ability to achieve its objectives is set out in the Corporate Plan and other supporting documentation such as Business Plans and risk registers.

2.7 Revenue Scotland expects management to take action to avoid or, where appropriate, mitigate the effects of those risks that are considered to exceed Revenue Scotland's risk appetite. Where a risk is deemed to exceed Revenue Scotland's risk appetite it will be captured in the corporate risk register along with the actions being taken to mitigate the risk.

2.8 The active, on-going commitment and full support of the Revenue Scotland Board through the work of the Audit and Risk Committee and Revenue Scotland Senior

Management Team is a necessary and essential part of this policy. Management will ensure that effective mechanisms are in place for assessing, monitoring and responding to any risks arising whilst the Revenue Scotland Board have ultimate responsibility for Risk Management.

2.9 All employees are expected to have an understanding of the nature of risk within Revenue Scotland and of the organisation's risk appetite. Where Revenue Scotland has delegated functions to other bodies, the risks associated with carrying out those functions will lie with the delegate body except where alternative arrangements, e.g. for financial risks, are set out in the relevant Memorandum of Understanding. It is the responsibility of the Revenue Scotland Senior Management Team to raise significant risks impacting 'other bodies' that could affect delivery of Revenue Scotland's Aims and Objectives, on the Corporate Risk Register.

3. Risk management approach

3.1 Overview of risk management

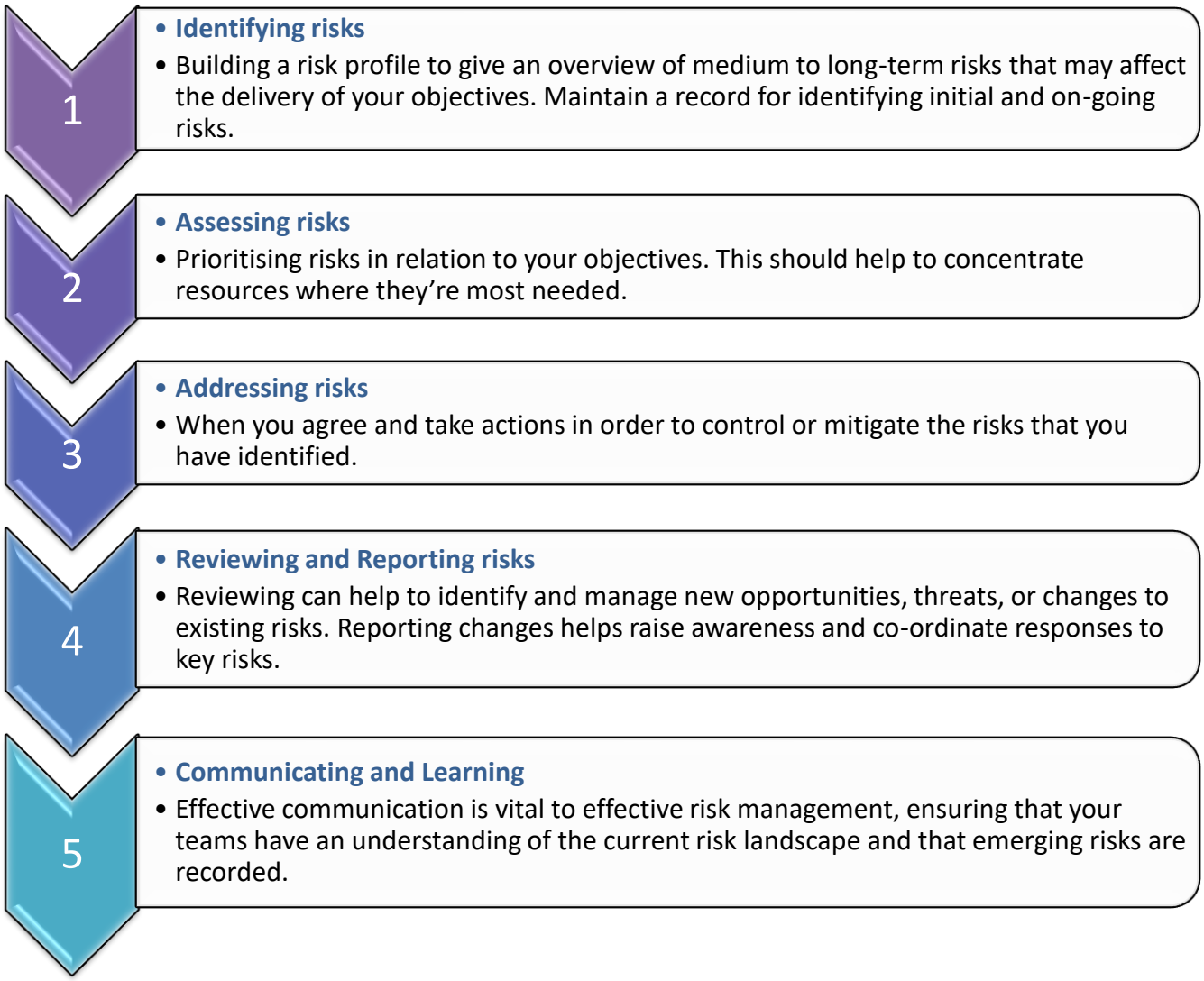
3.1.1 Revenue Scotland is committed to achieving its aims as defined in the Corporate Plan and Business Plan. In doing so, Revenue Scotland recognises that it will face a variety of risks. The task of management is to respond to these risks effectively so as to maximise the likelihood of Revenue Scotland achieving its objectives and ensuring the best use of resources.

3.1.2 Risk is defined as:

> ***'A quantifiable level of exposure to the threat of an event or action that will adversely affect Revenue Scotland's ability to achieve its objectives successfully.'***

3.1.3 We use risk management to systematically identify, record, monitor and report risks to enable the organisation to meet its objectives and to plan actions to mitigate those risks.

3.1.4 In order to help manage risk therefore, we employ a straightforward methodology which observes these 5 key steps:



3.2 Risk management objectives

3.2.1 To assist in the management of business and organisational risk the following objectives have been identified. These form the basis of Revenue Scotland's Risk Management Strategy:-

- Promote awareness of business and organisational risk and embed the approach to its management throughout the organisation.
- Seek to identify, measure, control and report on any business and organisational risk that will undermine the achievement of Revenue Scotland's business priorities, both strategically and operationally, through appropriate assessment criteria.

3.3 Risk management vision

3.3.1 Revenue Scotland will aim to identify risks and their causes at the earliest opportunity; measure the risk effect on the organisation; and put in place controls to mitigate risks.

3.3.2 Additionally, Revenue Scotland will seek to obtain assurance that the controls relied on to mitigate the key risks are effective. An assurance framework has been developed to support the on-going monitoring of controls (see under "monitoring and control").

3.4 Risk management culture

3.4.1 Revenue Scotland recognises the value of a risk management culture to the protection of taxpayer confidentiality and service.

Consequently, it will:-

- Review the Corporate Plan on an annual basis;
- Review corporate risk register on a quarterly basis;
- Integrate risk management with planning and delivery;
- Implement and monitor risk management arrangements across the organisation;
- Devolve responsibility for risk ownership and management as appropriate;
- Ensure that designated individuals receive the necessary training, on-going support and advice in connection with risk management; and
- Measure progress in its approach to risk.

3.5 Risk management structure

3.5.1 To ensure that Revenue Scotland has a full understanding of the risks being faced and the implications for the organisation, risks will be identified and assessed at three levels:-

Corporate: Those business risks that, if realised, could have a significant detrimental effect on Revenue Scotland's key business processes and activities, including reputational and financial risks.

Operational: Those business risks that, if realised, could have a significant detrimental effect on the key operational objectives and activities.

Project / Programme: Those business risks that, if realised, could have a significant detrimental effect on the outcome of a Programme or Project.

3.6 Responsibilities

3.6.1 The Revenue Scotland Board, through the Audit and Risk Committee, has ultimate responsibility for the management of the organisation's risks. The Accountable Officer is responsible for making sure that effective risk management processes are in place.

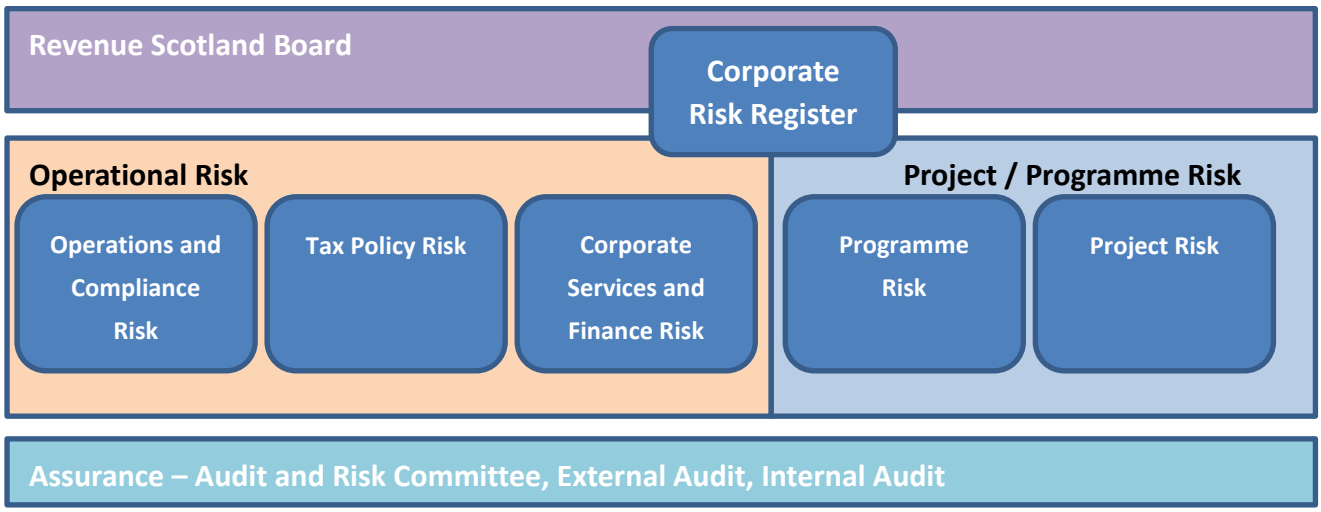
3.6.2 Everyone, however has a role to play in managing risk effectively. Our structure and governance framework supports this by providing both internal and external assurance.

3.6.3 It is helpful to have a nominated individual(s) from each team and/or functional area that have the responsibility to ensure that systems and processes are in place to review and report on relevant risks effectively: ensuring risk management information is maintained and communicated. This includes assuring themselves that effective risk reporting arrangements are established and maintained across all programmes of activity.

3.6.4 To support this, each team or project/programme should maintain a risk register and review it regularly.

3.6.5 The role of the Governance Team is to facilitate and support effective risk management practices throughout the organisation. This includes maintaining guidance and providing training for staff.

Diagram 2 describes where ownership and assurance.



3.7 Responsibilities

3.7.1 The risk registers shall follow a standard format (refer **Appendix 1**) and include the following elements:-

- A risk description;
- Controls in pace to mitigate risks;
- Current risk assessments of impact and likelihood;
- Controls confidence level;
- Target risk score; and
- Date – the date the risk was reviewed.

Corporate Risk Register: This register reflects the most significant risks that have the potential to impact on the ability of Revenue Scotland to meet its objectives as detailed in

the Corporate Plan. Revenue Scotland's Senior Management Team maintain this register; supported by the Head of Governance and the monthly Risk Management Group.

Operational Registers: The three operational teams must maintain their own risk registers which reflect the specific risks associated with their activities. Any 'red' risks, i.e. very high, should be evaluated to decide whether they merit inclusion in the corporate (strategic) risk register.

Programme / Project Risk Registers: A separate risk register must be maintained for each major programme and project. Any 'red' risks, i.e. very high, should be evaluated to decide whether they merit inclusion in the corporate (strategic) risk register.

4. Risk Management Process

4.1 Risk identification

4.1.1 This is the first step in building a risk profile, an overview of the medium to long-term risks that may affect the achievement of objectives.

4.1.2 It doesn't matter what method is used to identify risks but it is important to take a systematic approach to ensure a complete risk profile emerges as an outcome. For example, risks can be identified from a number of sources including:

- Audit activities;
- Management meetings;
- Working groups;
- Team meetings;
- Information from the media / publications;
- Horizon scanning;
- Recurring and ongoing complaints; and
- Changing legislation.

4.1.3 It is important, therefore, that risk features as a **standard agenda item** on all team meetings and working groups across Revenue Scotland. Any risks identified should be reported for inclusion in the relevant risk register.

4.1.4 A simple technique that provides a wide scan of areas that may affect objectives is a **PESTLES** analysis (see table below). Using **PESTLES** analysis categories to examine objectives will form a comprehensive risk profile for any given area of work.

POLITICAL		• Changes in policy; • Committee decisions; • Stakeholder relations.
ECONOMIC		• Financial constraints; • Effect of local economy; • Sustainability.
SOCIAL		• Preventative spend; • Demographic changes; • Staff implications.
TECHNOLOGICAL		• Obsolescence; • Cost of training and development; • Efficiency.
LEGAL		• Statutory Duties; • Procurement processes; • Accounting rules.
ENVIRONMENTAL		• Climate change implications; • Changing environmental standards.
SECURITY		• Physical assets; • Information security; • Data protection.

4.1.5 Reputation risk is included across the **PESTLES** categories. You will also notice that some of the examples on previous page could be relevant in more than one area e.g. data protection. It is important that risks are not narrowly categorised, **PESTLES** is a tool to aid the risk identification that will flow from the breadth of knowledge and information available on the subject at hand. A guide to risk descriptions is also provided at **Appendix 4**.

4.2 Analysing and assessing risk

4.2.1 A risk is assessed on the combination of the consequences of an event (**impact**) and its probability (**likelihood**). The following tables provide a guide to risk levels and how they should be recorded.

IMPACT - This is the estimated effect of the risk on the objective(s) in question. This is focused on scale, scope and resource implications.

IMPACT	CRITERIA
50 Very High	Destructive and unacceptable impact on objectives that would result in a major change to overall approach. Potentially large resource consequences that outweigh current operational circumstances.
25 High	Significant and unacceptable impact on objectives that would require a material change to critical approach/ procedure/process. Resource implications would be challenging to absorb within current operational circumstances.
10 Medium	Moderate impact on objectives that may require multiple changes in approach/procedure/process. Acceptable level of resource consequences.
5 Low	Minor impact on objectives, requires little overall change in approach. Few resource consequences.
1 Negligible	No real impact on achieving objectives.

Likelihood - This is the estimated chance of the risk occurring. This is focused on probability.

LIKELIHOOD	CRITERIA
5 Very High	>75% chance of occurring – almost certain to occur
4 High	51-75% chance of occurring – more likely to occur than not
3 Medium	26-50% chance of occurring – fairly likely to occur
2 Low	6-25% chance of occurring – unlikely to occur.
1 Negligible	1-5% chance of occurring – extremely unlikely to occur

4.2.2 The following tables provide a guide to the overall risk level based on multiplying the assessment of the impact and likelihood of a risk.

IMPACT	RISK PROFILE				
VERY HIGH	50	100	150	200	250
HIGH	25	50	75	100	125
MEDIUM	10	20	30	40	50
LOW	5	10	15	20	25
NEGLIGIBLE	1	2	3	4	5
LIKELIHOOD	RARE	LOW	MEDIUM	HIGH	VERY HIGH

RISK LEVEL	SCORE	RISK LEVEL DESCRIPTION
VERY HIGH	**100-250**	**Rating**: Unacceptable level of risk exposure that requires immediate mitigating action. **Reporting**: A decision should be taken whether to report the risk to Accountable Officer/Audit and Risk Committee.
HIGH	**40-75**	**Rating**: Unacceptable level of risk which requires controls to be put in place to reduce exposure. **Reporting**: A decision should be taken as to whether risks recorded as high should be escalated. Scores between 40 and 50 would not usually be escalated where scores of 75 should be given careful consideration.
MEDIUM	**10-30**	**Rating**: Acceptable level of risk exposure subject to regular active monitoring. **Reporting**: At operational level.
LOW	**1-5**	**Rating**: Acceptable level of risk subject to regular passive monitoring. **Reporting**: At operational level. Consideration should be given as to whether risks recorded as low are still extant.

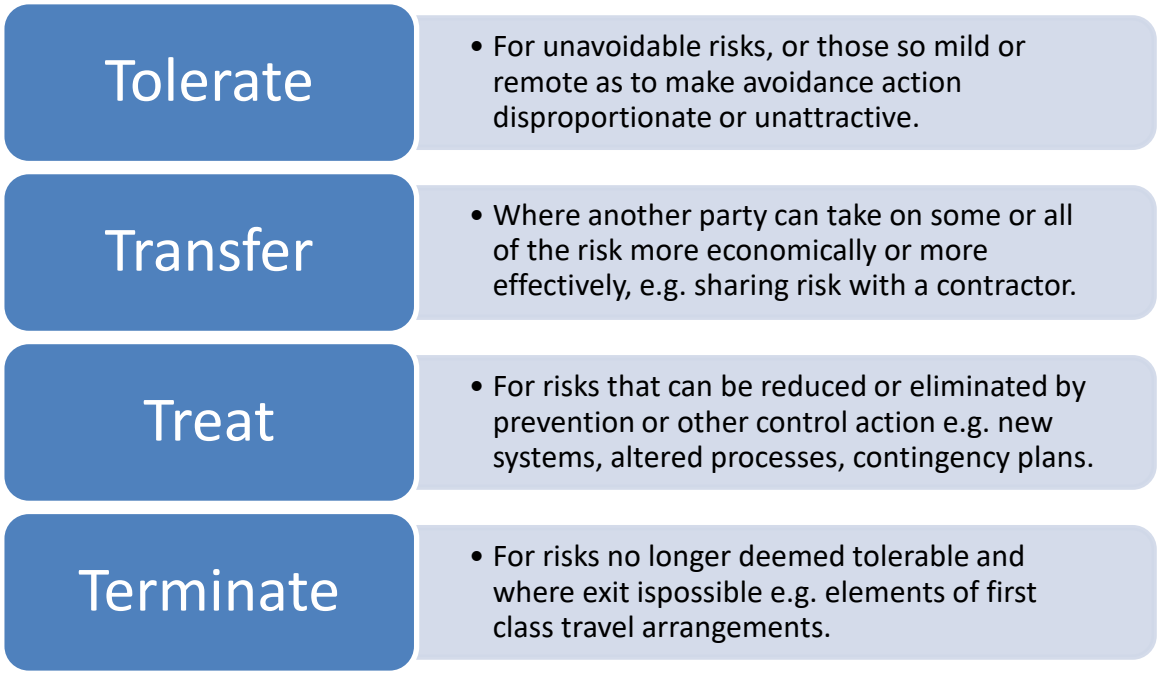
4.2.3 The risk level descriptions above are for strategic, corporate risk reporting. Teams would report up, or escalate, to the strategic level. Programmes and projects should have dedicated governance arrangements in place to allow for upward reporting.

4.2.4 For escalation, management judgement is required based on the nature and scale of the specific risk e.g. the risk of a key member of a project leaving may be very high but not of a sufficient scale in terms of scope to require escalation. The risk management framework is reliant on the judgement of those responsible for risk when escalating risks through the organisation's risk management structure.

4.3 Addressing risk

4.3.1 Once risks have been identified and assessed, the next stage is to decide what action needs to be taken to address the highlighted risks.

4.3.2 Risks can be dealt with in four main ways, depending on the kind of challenge they present according to how likely they are to occur, and the impact if they did occur. In choosing between these responses, factors to consider include, cost, feasibility, probability, and the potential impact. Responses to risk can be to:



4.3.3 It is important to recognise that excessive caution can sometimes be as damaging as unnecessary risk-taking. There may be opportunities to exploit a positive impact that might arise whenever tolerating, treating, transferring or terminating a risk i.e. where the potential gain seems likely to outweigh the potential downside.

4.3.4 The following examples illustrate how threats can be viewed as opportunities, they still need controls and actions to manage them, but allow you to think more creatively about how uncertainty can be managed and viewed in a more positive light.

THREAT	OPPORTUNITY
Staff numbers are reducing and new IT systems require investment and training.	We work more flexibly and make better use of technology to aid staff development and operational efficiency.
New powers are being devolved to the Scottish Government, requiring new knowledge and skills, robust planning and implementation.	We demonstrate competence in government to strengthen reputation with stakeholders e.g. stamp duty and landfill tax.
Budgets have been reduced to a level requiring creativity to maintain service levels. This needs a framework and incentives to make it work.	Current financial constraints are used as an energising factor to explore new areas of work and approaches.
Shared service coverage does not maximise resources and is difficult to maintain. Several public sector organisations are not engaged effectively.	More upfront investment to engage the wider Scottish public sector in extending shared service coverage: reducing costs and aiding efficiency targets.

4.4 Reviewing and Reporting Risk

4.4.1 The Risk Register and Risk Card templates provided at **Appendix 1 and 2** should be used at operational levels and above. It should also be considered when programmes and projects are developing their own arrangements.

4.4.2 When escalating risks to the corporate level you will, however need to ensure that your risk information complies with the corporate template. The corporate template uses 'Controls Confidence' this allows reporting of the assurance levels of the current controls and the level of confidence actions planned will manage the risk sufficiently to meet its target score and date.

4.4.3 Other methods you may wish to consider:

- **RISK ACTIVITY** – a way of reporting the amount of activity being undertaken to manage and mitigate the particular risk – this is usually a helpful method if risk scores are quite often static.

- **EXCESS RISK** – highlights the difference between the current and target risk scores – this is a helpful tool to understand your risk appetite against your risk and the gap required to manage the risk effectively.

4.4.4 Risks should be reviewed on a regular basis and the Risk Cards updated in line with agreed and established reporting arrangements. The Risk Register should be used as a tool for reporting and not the repository for all the information regarding a particular risk, the register should primarily be used as a catalyst for helpful and productive discussion and onward action. The Risk Cards, by design, offer a greater opportunity to develop controls and actions – updating these regularly to ensure that the detail provided is timely, relevant and accurate.

4.4.5 In particular, when developing your Risk Cards you should consider the **RULE OF FIVE**. This is about sensibly reducing down the amount of detail that is provided in the controls in place and actions planned sections of the register to five (or less) key bullet points for each risk. Ensuring that the cards are a prompt for discussion. Risk owners should have the requisite knowledge of a risk to provide further details if questioned. The actions planned section should also detail key dates against each bullet point providing a more direct link between the target score and target date entries but also providing a much clearer link to where you are (controls in place) and where you are heading (actions planned) on your risks. Target dates should also reflect the dates detailed in the actions planned.

Risk Management Maturity

4.4.6 A key aspect of monitoring and reporting progress is the establishment of a Risk Maturity Model. This model provides senior management with a snapshot of where the risk processes and principles that Revenue Scotland employs have led to changes and progression in risk management. It provides assurance that risk management processes are fit for purpose and also identifies areas where further improvement is required. Revenue Scotland's risk maturity model is attached as **Appendix 3**.

4.4.7 The risk maturity model will be reviewed annually by the Revenue Scotland Senior Management Team and they will report findings and any actions to raise 'maturity' in areas of poorer performance to the Audit and Risk Committee and for subsequent approval by the Revenue Scotland Board.

4.5 Assessing Risk Confidence

4.5.1 When assessing the requisite confidence levels for any given area, consider the size, scope and resource implications of any control weaknesses.

SUBSTANTIAL - Controls are robust and well managed

Processes and procedures are effective in supporting the delivery of any related objectives. Any exposure to potential weakness is low and the materiality of any consequent risk is negligible.

e.g. The identification and recording of key business risks is part of regular management discussions that are linked to business objectives and performance monitoring arrangements.

REASONABLE - Controls are adequate but require improvement

Some improvements are required to enhance the adequacy and effectiveness of processes. There are weaknesses in the procedures in place but not of a significant nature.

e.g. The identification and recording of key business risks is part of business planning processes but discussions are quarterly and not linked to decision-making activities.

LIMITED - Controls are developing but weak

There are weaknesses in the current processes in place that either are, or could, affect the delivery of any related objectives. Exposure to the weaknesses identified is moderate and being mitigated.

e.g. The identification and recording of key business risks is undertaken but it is not directly linked to business planning or revisited on a regular basis. An issue related to risk monitoring and reporting may have arisen in-year.

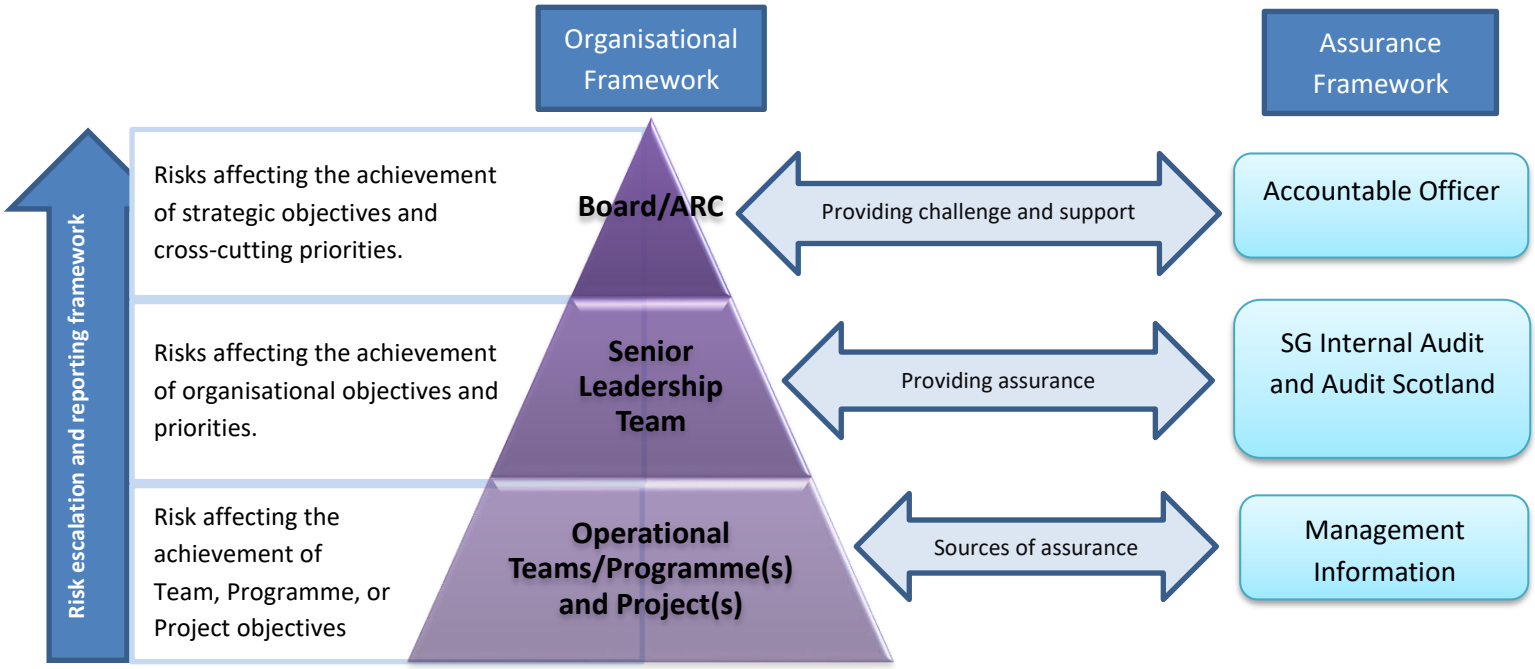
INSUFFICIENT - Controls are not acceptable and have notable weaknesses

There are significant weaknesses in the current procedures, to the extent that the delivery of any related objectives are at risk. Exposure to the weaknesses identified is sizeable and requires urgent mitigating action.

e.g. The identification and recording of key business risks is undertaken but not at sufficient level or detail. It is discussed on an ad-hoc basis. An important issue related to risk monitoring and reporting may have arisen in-year.

4.6 Risk Escalation

4.6.1 The framework here is designed to provide effective support and challenge in managing your risks. Escalating a risk to the next level does not remove responsibility for managing the risk from the business area but ensures its effective communication, increasing awareness and highlights where more supportive action is needed.



Considering Escalation

4.6.2 To highlight risks appropriate for more senior awareness or action there is a structure in place for upward reporting, depending on the level of risk. You can also choose

to escalate to more than one forum for example a relevant subject area board or assurance meeting (for example, SLT or Staffing and Equalities Committee (SEC)).

4.6.3 When considering whether escalating a risk is the right thing to do, consider appropriate risk tolerances that may be in place. Risk tolerance and its assessment is not an exact science, bur provided below is three easy steps to considering escalation.

SCALE - Is it sufficiently damaging to objectives?

SCOPE - Does it cut across several areas of work?

RESOURCES - Can it be described as exceptional?

4.6.4 Escalation should be based on the judgement of the nature and scale of the specific risk e.g. the risk of a key member of a project leaving may be very high but not of sufficient scope to require escalation.

4.6.5 Escalation should not be decided by risk scoring alone, but through detailed discussion to enable effective action. The risk framework is reliant on the judgement of those responsible for risk. Escalating a risk to this level can ensure increased visibility and enable more senior support and challenge ensuring a comprehensive perspective on the risk and facilitating more connections that can support delivery.

4.7 Communication and Learning

4.7.1 Managing risk is not about Risk Registers and Risk Cards, but about the achievement of objectives. Everyone, all the way up to the Board has a clear role to play in establishing that risk culture (paragraph 3.4 onwards refers). Working together, learning from our experiences will help to establish and maintain that positive risk culture

4.7.2 Different perspectives on risk are extremely valuable so this should be promoted - people view risk differently, team members, programme boards, senior management, stakeholders and the public.

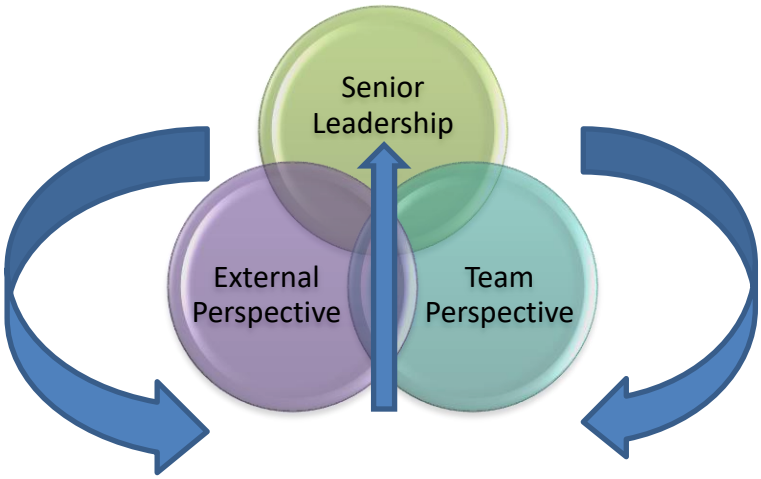
4.7.3 Ensuring that we tap into these diverse views and utilise other people's experiences and perspectives can help us to identify and manage our risks better. Here are some quick and easy steps to follow:

1. **UTILISE DIVERSE PERSPECTIVES** in your teams, projects or programmes and think about what arrangements are in place in your area to ensure that risk information is supporting your decision–making.

2. **FEEDBACK** – are you sharing what has been done with your teams, following risk identification and risk escalation?

3. **ARE YOU SHARING THE LEARNING** – allowing your teams to benefit from lessons learned in a project or programme?

COMMUNICATION FEEDBACK LOOP



5. Risk Appetite

5.1 Risk appetite is an expression of how much risk Revenue Scotland is prepared to take. Those involved in risk evaluation and prioritisation should, when considering risk, discuss and express the risk appetite as they see it.

5.2 The Risk Cards prompts risk owners to consider risk appetite when updating a risk information and mitigating controls/actions. They need to consider not only the risk score before and after existing mitigating action but also the final tolerable risk status (i.e. what they are aiming for in terms of status for that particular risk).

5.3 Revenue Scotland's risk appetite is summarised in the following table. This table describes the different levels of risk appetite and the likely approach you would take to the management of risks as a result of that appetite.

Risk Appetite

RISK APPETITE	DESCRIPTIONS
VERY LOW/ AVERSE	Avoidance of risk in achievement of key objectives is paramount. Activities undertaken will only be those considered to carry little inherent risk e.g. around statutory requirements.
LOW/ MINIMALIST	Tendency to undertake activities that are considered safe in achieving objectives. There should be a low degree of inherent risk. The pursuit of opportunity is not a key driver in this area.
MEDIUM/ CAUTIOUS	Willingness to accept a degree of risk in order to achieve key delivery objectives. Particularly where the opportunity of significant gains has been identified. Inherent risk is deemed controllable to a large extent.
HIGH/OPEN	Aim to undertaken activities that have a high degree of value for money, the likelihood of success being a determining factor. These activities may potentially carry a large amount of residual risk.
VERY HIGH/ HUNGRY	There is an eagerness or requirement to be innovative and a focus on activities designed to maximise opportunity. This approach will carry with it very high residual risk in pursuit of very high reward.

Appendix 1 - Corporate Risk Register Format

Risk No	Risk Name	Risk Description	Risk Owner	Risk Manager	Risk Appetite	Current Impact	Current Likelihood	Current Risk Score	Controls Confidence Level	Target Impact	Target Likelihood	Target Risk Score	Target Date
1						1	2	**2**	**Substantial**	1	5	**5**	
2	Resourcing and capability development	**IF**: We fail to recruit and retain highly knowledgeable, skilled staff. **THEN**: We will lose key capabilities, have reduced capacity, make defective decisions and more mistakes, and increase pressure and workload on remaining staff.	Chris Myerscough	Deirdre Watt	Very Low/Averse	5	2	**10**	**Insufficient**	5	4	**20**	
3						10	3	**30**	**Limited**	10	3	**30**	
4						25	4	**100**	**Reasonable**	25	2	**50**	
5						50	5	**250**	**Insufficient**	50	5	**250**	
6						25	3	**75**	**Substantial**	50	1	**50**	

RS Risk Register Template.xlsm

The risk register format above is based on an internationally recognised risk register model. The content has been kept simple and is in Excel format for flexible reading and reporting. This is a standard format for risk registers across the Scottish Government. Standardisation enables an accurate comparison and contrast of risks across the office, as well as improved information flows on risk in the organisation.

RISK No: Is a helpful reference to aid reporting.

RISK NAME: A suitable name that relates to the description

RISK DESCRIPTION: Should be a short summary of the risk, focussing on cause and impact i.e. what is the specific area at risk and how will it impact on objectives.

RISK OWNER: A member of SLT (who is not the CEO) that has been delegated overall responsibility for a risk

RISK MANAGER: The designated day to day manager of the risk – delivering its mitigating actions and managing/implementing relevant controls

RISK APPETITE: An expression of how much risk Revenue Scotland is prepared to take.

CURRENT RISK IMPACT AND LIKELIHOOD: This is the assessment of the impact/likelihood of a risk after the controls in place have been applied. Impact on a scale 1-50: 1 – Negligible, 5 – Low, 10 – Medium, 25 – High, 50 – Very High. Likelihood on a scale 1-5: 1 – Rare, 2 – Low, 3 – Medium, 4 – High, 5 – Very High.

CURRENT RISK SCORE: This is the overall assessment of the level of risk exposure after controls in place have been applied calculated by multiplying the impact and the likelihood scores: 1-5 Low, 10-30 Medium, 40-75 High, 100-250 Very High. This gives a useful picture of how well controls are currently operating and to what degree the risk still needs to be monitored.

CONTROLS CONFIDENCE: This allows reporting of the assurance levels of the current controls and the level of confidence actions planned will manage the risk sufficiently to meet its target score and date.

TARGET RISK IMPACT AND LIKELIHOOD: This should be an assessment of the target impact/likelihood that should be aimed for; where risk is at an acceptable level and the cost of managing the risk does not outweigh the benefit to objectives.

TARGET RISK SCORE: This is an overall assessment of the desirable target risk score – considering the tolerance for risk (in any given area) and the effective use of resources in trying to achieve successful outcomes. Once this score is achieved then the risk should be re-examined, whether it should be restated or actively monitored.

TARGET DATE: This is a specified target date by which to achieve the target risk score. Where this date is exceeded and target scores have not been met the risk should be reviewed and assessments altered as required.

Appendix 2 - Risk Profile Card

Date updated – [Day/Month/Year]

Risk No and Name	
Corporate Plan 2018-21 Objective(s)	
Risk Description	
Risk Owner/Manager	

Current Risk Assessment	**Target Risk Assessment**
Impact V High 50 100 150 200 250 High 25 50 75 **100** 125 Med 10 20 30 40 50 Low 5 10 15 20 25 Neg 1 2 3 4 5 Likelihood	Impact V High 50 100 150 200 250 High 25 50 **75** 100 125 Med 10 **20** 30 40 50 Low 5 10 15 20 25 Neg 1 2 3 4 5 Likelihood
Risk Appetite	
Controls Confidence	
Risk Management	**Treat** Telerate Transfer Terminate

	Actions	**Owner**	**Due**
Mitigating Actions			

Additional Risk Information

HOW would this risk happen?
•
WHAT would the potential impact/outcome be?
•
WHAT early warning indicators exist?
•
WHAT controls are in place?
•

Appendix 3 - Risk Maturity Model

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
Enabled	Risk management and internal control is fully embedded into operations. All parties play their part and have a share of accountability for managing risk in line with their responsibility for the achievement of objectives.	There are processes for identifying and assessing risks and opportunities on a continuous basis. Risks are assessed to ensure consensus about the appropriate level of control, monitoring and reporting to carry out. Risk information is documented in a risk register.	Responses to the risks have been selected and implemented. There are processes for evaluation risks and responses implemented. The level of residual risk after applying mitigating controls is accepted by the organisation, or further mitigations have been planned.	High quality, accurate and timely information is available to operational management and directors. The board reviews the risk management strategy, policy and approach on a regular basis, e.g. annually, and review key risks, emergent & new risks, and action plans on a regular basis.	The organisational performance management framework and reward structure drives improvements in risk management. Risk management is a management competency. Management assurance is provided on the effectiveness of their risk management on a regular basis.
Managed	Risk management objectives are defined & managers are trained in risk management techniques. Risk management is written into performance expectations of managers. Management and executive level of responsibilities for key risks have been allocated.	There are clear links between objectives and risks at all levels. Risk information is documented in a risk register. The organisation's risk appetite is used in the scoring system for assessing risks. All significant projects are routinely assessed for risk.	There is clarity over the risk level that is accepted within the organisation's risk appetite. Risk responses are appropriate to satisfy the risk appetite of the organisation have been selected and implemented.	The Board reviews key risks, emergent and new risks, and action plans on a regular basis. It reviews the risk management strategy, policy and approach on a regular basis (annually). Senior Managers will require interim updates from delegated managers on individual risks which they have personal responsibility.	The organisation's risk management approach and the Board's risk appetite are regularly reviewed and refined in light of new risk information reported. Management assurance is provided on the effectiveness of their risk management on an ad hoc basis. The resources used in risk management are become quantifiably cost effective. Measures are set to improve certain aspects of risk management activity e.g. number of risks materialising or surpassing impact – likelihood expectations.

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
Defined	A risk strategy and policies are in place and communicated. The level of risk taking that the organisation will accept is defined and understood in some parts of the organisation, and it is used to consider the most appropriate responses to the management of identified risks. Management and executive level of responsibilities for key risks have been allocated.	There are processes for identifying and assessing risks and opportunities in some parts of the organisation but not consistently applied in all. All risks identified have been assessed with a defined scoring system. Risk information is brought together for some parts of the organisation. Most projects are assessed for risk.	Management in some parts of the organisation are familiar with, and able to distinguish between, the different options available in responding to risks to select the best response in the interest of the organisation.	Management have set up methods to monitor the proper operation of key processes, responses, and actions plans. Management report risks to directors where responses have not managed the risks to a level acceptable to the Board.	The Board gets minimal assurance on the effectiveness of risk management.
Aware	There is a scattered, silo-based approach to risk management. The vision, commitment and ownership of risk management have been documented. However, the organisation is reliant on a few people for the knowledge, skills and the practice of risk management activities on a day-to-day basis.	A limited number of managers are trained in risk management techniques. There are processes for identifying and assessing risks and opportunities, but these are not fully comprehensive or implemented. There is no consistent scoring system for assessing risks. Risk information is not fully documented.	Some responses to the risks have been selected and implemented by management according to their own perception of risk appetite in the absence of a board-approved appetite for risk.	There are some monitoring processes and ad hoc reviews by some managers on risk management activities.	Management does not assure the Board on the effectiveness of risk management.

	Risk Governance	Risk identification & assessment	Risk mitigation & treatment	Risk reporting & review	Continuous improvement
Naive	No formal approach developed for risk management. No formal consideration of risks to business objectives, or clear ownership, accountability and responsibility for the management of key risks.	Processes for identifying and evaluating risks and responses are not defined. Risks have not been identified nor collated. There is no consistent scoring system for assessing risks.	Responses to the risks have not been designed or implemented.	There are no monitoring processes or regular reviews of risk management.	Management does not assure the Board on the effectiveness of risk management.

Appendix 4 – Guide to Risk Descriptions

Risk is the uncertainty that may impact either positively or negatively on the achievement of objectives. In describing a risk for monitoring and reporting, it is helpful to consider cause and effect when defining a risk. This can focus the discussion on what action is required to manage a risk effectively.

At the corporate level a progressive approach to describing risks should be taken – focussing on opportunities and presenting a more positive analysis of risk information. When developing the relevant arrangements you should consider the cause and effect, and ensure a consistent focus on the key phase of risk management: the actions being taken to achieve objectives.

To represent the cause and effect, risk descriptions can be seen as a combination of **'if'** and **'then'** for example;

> **If:** [Cause] Key stakeholders are not engaged with their role in supporting delivery arrangements...
>
> **Then:** [Effect] ...it will result in increased programme costs.

Risk descriptions should be written to clearly describe what it is you are really worried about. See the examples offered through the following table:

Risks are not	The same risk more clearly described
Questioning the objective; “Delivering the change programme might not be the best way to drive efficiency”	**IF:** We don’t have a clear evaluation plan for the programme **THEN:** this will mean we can’t test the level of efficiencies at key stages
One-word Risks; “Fraud”, “Fire”, “Reputation”	**IF:** We fail to have effective separation of duties **THEN:** this will increase the risk of fraud in our systems **IF:** We don’t have an appropriate evacuation plan in place **THEN:** in the event of a fire we can’t ensure staff know what they need to do **IF:** We don’t have a stakeholder communications and engagement plan **THEN:** this will risk relations with key groups if they are not engaged on key issues
Statements of fact; “There is a risk that projects may fail”	**IF:** We don’t have clear plans in place with good embedded risk management processes **THEN:** the likelihood of project failure is high
Failure to…; “recruit enough staff”	**IF:** We don’t have a clear resource and recruitment plan in place **THEN:** we can’t ensure that we can recruit enough staff to deliver programme
Incidents; “Due to the computer system crashing……”	**IF:** We don’t have effective back-up systems in place **THEN:** in the event of a malfunction we may not be able to restore service as soon as possible

Risks can be expressed either negatively or positively depending on your preference, just ensure that whichever method you choose you apply it consistently.

A positively articulated risk using the first risk example above could read;

IF: We have a clear evaluation plan for the programme

THEN: this will enable us to test the level of efficiencies made at key stages.