

RISK MANAGEMENT

The Scottish Government Guide

Created by the Governance and Risk Team on
behalf of the Scottish Government Risk Champion
April 2018



Scottish Government
Riaghaltas na h-Alba
gov.scot

FOREWORD

“

Risk is essential to deliver effective change, progress and success.

The greatest benefit will often be delivered by an approach that is less obvious or an idea that is more creative and a path that presents significant risk. It is by managing risk in pursuit of our priorities that will maximise opportunities and improve outcomes.

Managing risk is everyone's responsibility and it is built into our competency framework, our project and programme management and our approach to government.

This guide to risk management has been developed to support you in thinking through your challenges and taking effective risk-based decisions.

It is vital that we all work to improve the richness of the discussions we have about risks and opportunities. We are not saying you have to be risk averse, but focus on the outcome required. This guide will help you navigate a structured approach to your work, and to develop a level of sound judgment to make the right choices.

”

DG Scottish Exchequer – Scottish Government Risk Champion



CONTENTS

Managing
risk



Before you begin



What is the Scottish
Government process?



Identifying
your risks



Assessing
your risks



Addressing
your risks



Reviewing and
reporting



Quick
guides



MANAGING RISK

A risk is anything that can impede or enhance our ability to meet our current or future objectives and the achievement of the Scottish Government's priorities captured by the National Performance Framework.

Managing our risk effectively is very important. It helps us to make the most of opportunities, deliver our objectives and protect the interests of our stakeholders.

Managing risk is everyone's responsibility and therefore it is built into our competency framework, our programme and project management arrangements and our directorate planning processes.

This guidance covers all stages of risk management from planning to reporting and communications. This is a defined framework which outlines good practice on how to clarify your objectives, identify, assess, address, review, report and communicate your risks. There are also helpful guides on understanding your risk appetite, understanding risk escalation routes and tools for recording risk information.

This approach is supported by the Governance and Risk team that works to:

- develop the Scottish Government risk management framework
- provide advice and guidance on risk management
- deliver training and workshops

For further support email GovandRisk@gov.scot

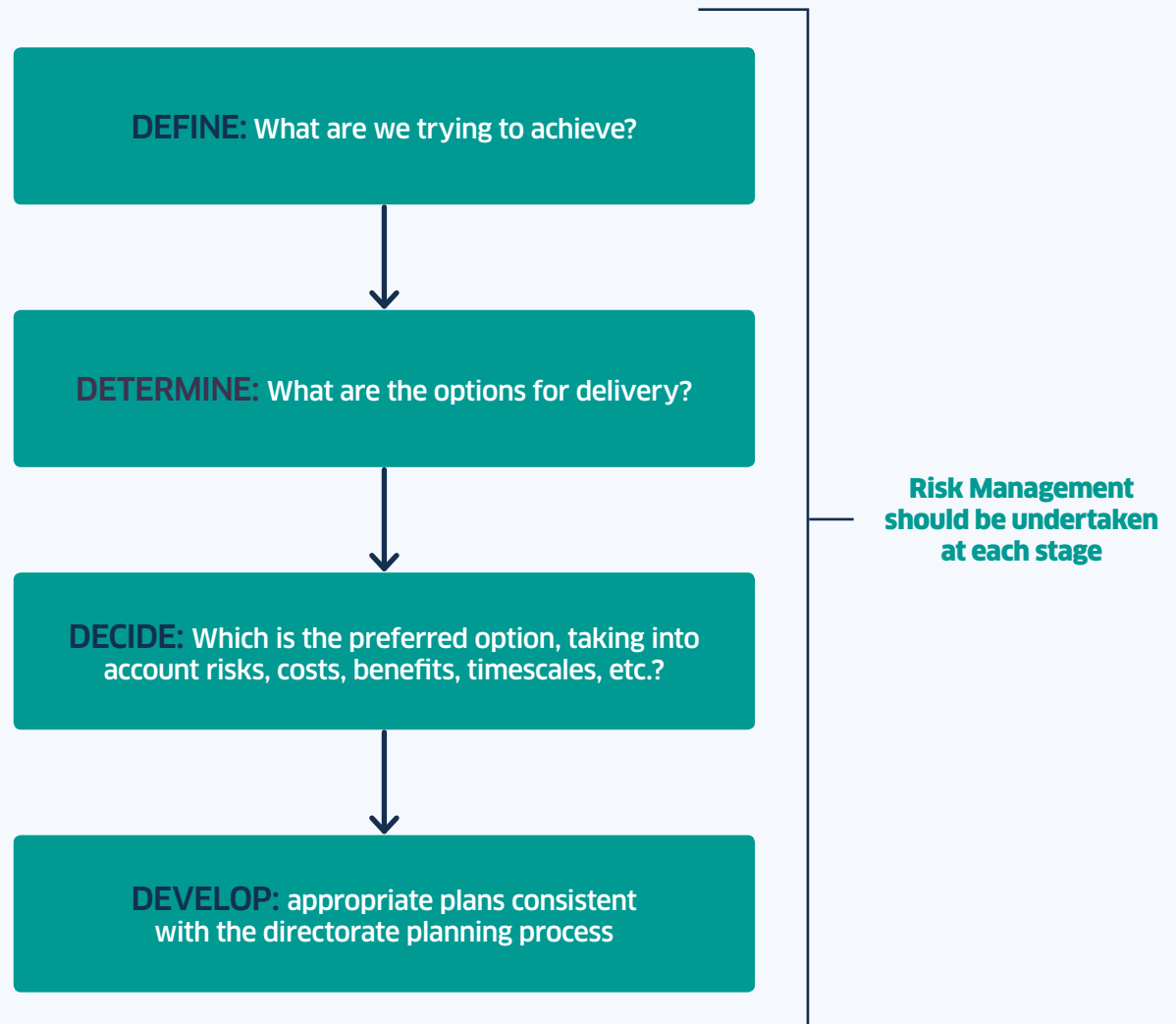
Further resources to support you can be found at Links to other [resources page](#) of this guide.



BEFORE YOU BEGIN

To manage your risks effectively you must first clarify and understand the objectives that you are trying to achieve. (This should be at the relevant level e.g. as a Directorate, Division, Team, Programme or Project).

Your objectives will be the focus of any risk management information, so risk identification needs to be undertaken with a clear strategy and clarity of purpose and is an important part of planning and managing performance and priorities effectively:



WHAT IS THE SCOTTISH GOVERNMENT PROCESS?

We have a straightforward methodology to help manage risk effectively and it follows these key 5 steps:

- 1. Identifying risks** Building a risk profile to give an overview of medium to long-term risks that may affect the delivery of your objectives. Maintain a record for identifying initial and on-going risks.
- 2. Assessing risks** Prioritising risks in relation to your objectives. This should help to concentrate resources where they're most needed.
- 3. Addressing risks** When you agree actions in order to control or mitigate the risks that you have identified.
- 4. Reviewing and Reporting risks** Reviewing can help to identify and manage new opportunities, threats, or changes to existing risks. Reporting changes helps raise awareness and co-ordinate responses to key risks.
- 5. Communicating and Learning** Effective communication is vital to effective risk management, ensuring that your teams have an understanding of the current risk landscape and that emerging risks are recorded.

This guide will take you through this 5 step process, providing tools and techniques to support you and key information to help you manage your risks effectively.

Communication and Learning

- 🔍 Identifying Risk
- ⚠️ Assessing Risk
- 📍 Addressing Risk
- 📄 Reviewing and Reporting Risk

Risk Environment

- 🏛️ Political
- 📈 Economic
- 👥 Social
- ⚙️ Technological
- ⚖️ Legal
- 🌿 Environmental
- 🔒 Security










IDENTIFYING YOUR RISKS

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.

It doesn't matter what method you use to help identify your risks but you should take a systematic approach to ensure you have a complete risk profile.

A simple technique that provides a wide scan of areas that may affect objectives is a PESTLES analysis (see the **Risk Framework** diagram on the previous page)

CATEGORY		EXAMPLES
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.

Using PESTLES analysis categories to examine objectives will form a comprehensive risk profile for a given area of work.

Check out the PESTLES risk assessment quick guide for examples of how you can assess your risks using the PESTLES framework

IDENTIFYING YOUR RISKS CONTINUED

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. See the **Risk Descriptions - a How to guide** once you have identified your risks.

Another simple method to help identify risk is to undertake a **SWOT** analysis on a particular piece of work, focusing on:

- **STRENGTHS:**
internal attributes that are helpful to achieving an objective.
- **WEAKNESSES:**
internal attributes that are harmful to achieving an objective.
- **OPPORTUNITIES:**
external conditions that are helpful to achieving an objective.
- **THREATS:**
external conditions that could be detrimental to performance.

For example:



These tools provide a quick and straightforward way of highlighting key factors in order for you to determine risks from small projects to strategic priorities.

ASSESSING YOUR RISKS

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 RARE	1-5% chance of occurring – extremely unlikely to occur

ASSESSING YOUR RISKS CONTINUED

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

ASSESSING YOUR RISKS CONTINUED

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 Committee level or Programme Board or for possible reporting to the Executive Team and Corporate Board.
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 directorate level.
LOW	1-5	Rating: Acceptable level of risk subject to regular passive monitoring. Reporting: At directorate level. Consideration should be given as to whether risks recorded as low are still extant.

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

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 Scottish Government **Risk Management Structure**.

ADDRESSING YOUR RISKS

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

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:

TOLERATE

For unavoidable risks, or those so mild or remote as to make avoidance action disproportionate or unattractive.

TREAT

For risks that can be reduced or eliminated by prevention or other control action e.g. new systems, altered processes, contingency plans.

TRANSFER

Where another party can take on some or all of the risk more economically or more effectively, e.g. sharing risk with a contractor.

TERMINATE

For risks no longer deemed tolerable and where exit is possible e.g. elements of first class travel arrangements.



ADDRESSING YOUR RISKS CONTINUED

Taking the Opportunity:

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.

These 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.

REVIEWING AND REPORTING

The Scottish Government risk template should be used at directorate level and above, it should also be considered when divisions, programmes and projects are developing their own local arrangements. When escalating risks to directorate level and above you will however need to ensure that your risk information complies with the corporate template. This can be found on the risk **intranet pages**.

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.

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.

Further information on the risk template can be found at quick guide 7

Further tools techniques and resources can be found later in this guide.

Risks should be reviewed on a regular basis and the risk register updated in line with local 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 RULE OF FIVE

When developing your risk register 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 register is 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.**

COMMUNICATION AND LEARNING

Managing risk is not about risk registers but about the achievement of objectives. Everyone, all the way up to the Permanent Secretary has a clear role to play in establishing that risk culture. Working together learning from our experiences will help to establish and maintain that risk culture

Different perspectives on risk are extremely valuable so bring them in!

People view risk differently, team members, programme boards, senior management, Ministers, stakeholders and the public.

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, division, directorate, project or programme 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



QUICK GUIDES

QUICK GUIDE 1

RISK DESCRIPTIONS

QUICK GUIDE 2

RISK INTERROGATION –
KEY QUESTIONS

QUICK GUIDE 3

HOW DO I ESCALATE
MY RISKS?

QUICK GUIDE 4

RISK APPETITE
AND TOLERANCE –
HOW DO I ASSESS IT?

QUICK GUIDE 5

PESTLES RISK ASSESSMENT

QUICK GUIDE 6

RISK REPORTING –
TOOLS & TECHNIQUES

QUICK GUIDE 7

USING THE TEMPLATE
RISK REGISTER

QUICK GUIDE 8

CONFIDENCE LEVELS –
WHAT DO THEY MEAN?

QUICK GUIDE 9

ROLES AND RESPONSIBILITIES

QUICK GUIDE 1 RISK DESCRIPTIONS – A HOW TO GUIDE

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 Executive Board take a progressive approach to describing risks – focussing on opportunities and presenting a more positive analysis of risk information.

When developing your 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.



QUICK GUIDE 1 RISK DESCRIPTIONS – A HOW TO GUIDE CONTINUED

Risk descriptions should be written to clearly describe what it is you are really worried about.

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 which ever 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.

QUICK GUIDE 2 RISK INTERROGATION – KEY QUESTIONS

When reviewing and reporting your risks, think about how effective discussion can help scrutinise and review your risks at management meetings etc. and what are the best lines of communication to ensure that relevant teams and colleagues are informed of further action, escalation and the general outcome of discussions.

When reviewing your risks here are some practical elements to think about:

- What are the key elements of the risk?
- What actions are in place/planned and what is the expected impact of each action?
- Will the risk be fully mitigated within the resources currently available, what more could be done, what further resources are required?
- Who needs to know about the risk?
- What is the timetable for reviewing the progress?

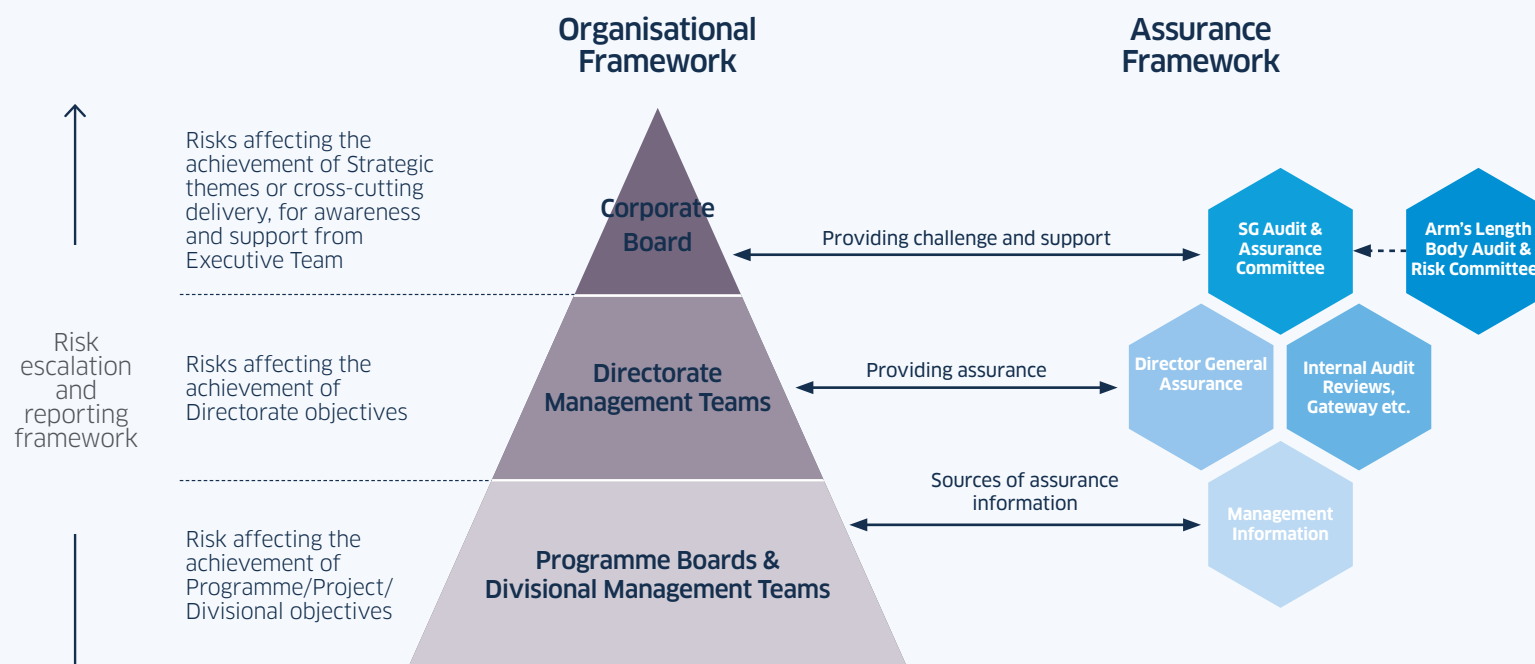
It can also be helpful to gain insight from colleagues not directly connected to the risk you are managing – consider asking an outside observer to gauge their opinion on the following questions:

- Are you doing enough to mitigate this risk and at the right pace?
- How will you know if the actions have had the intended effect?
- Who can help manage this if it is a cross-cutting risk?
- What contingency arrangements do you have in place should this risk occur?

QUICK GUIDE 3 HOW DO I ESCALATE MY RISKS?

Scottish Government Risk Management Structure

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.

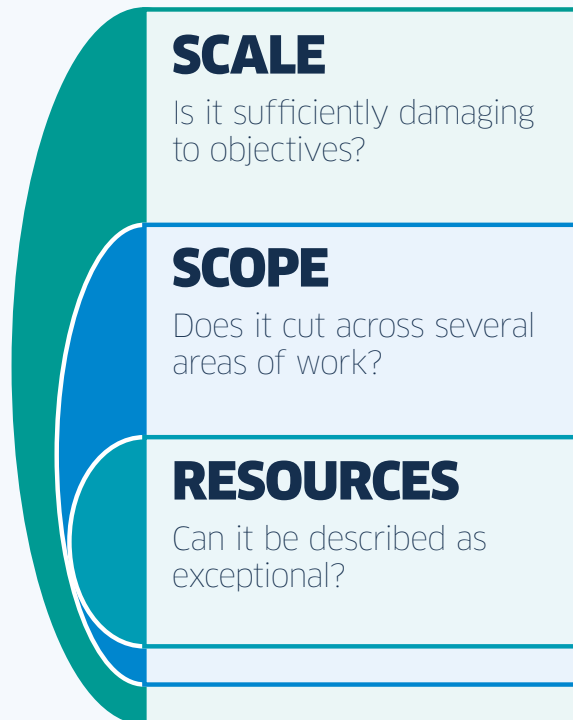


Considering Escalation

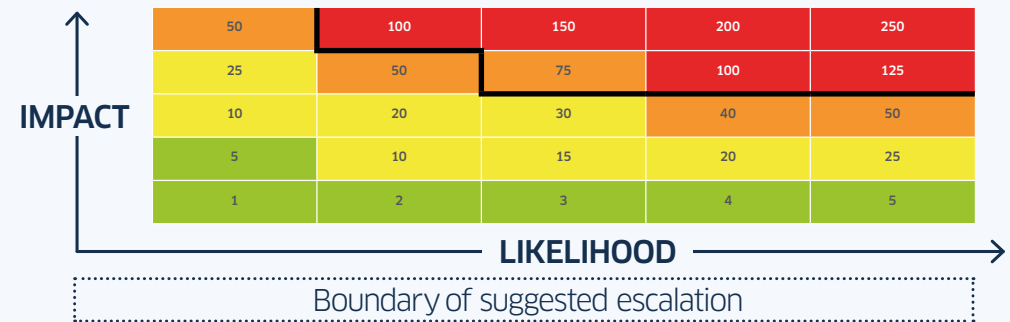
To highlight risks appropriate for more senior awareness or action there is a structure in place for upward reporting, depending on the level of risk. You can also choose to escalate to more than one forum for example a relevant corporate subject area board or assurance meeting.

QUICK GUIDE 3 HOW DO I ESCALATE MY RISKS? CONTINUED

Risk tolerance and its assessment is not an exact science. Here are three easy steps to considering escalation



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.



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.

QUICK GUIDE 4 RISK APPETITE AND TOLERANCE – HOW DO I ASSESS IT?

Your risk appetite is the levels and types of risk you are prepared to accept (and not accept) in achieving your objectives. Ensuring you understand your appetite for risk is essential. **Here are the 3 key steps to implementing an effective risk appetite.**

STEP ONE: Consider and develop your risk appetite.

You must take into account different viewpoints when considering the correct approach. Risk appetite will be different at different times, depending on the political environment for example, and in different projects and programmes. The tone needs to come from the top, taking into account Ministerial views, the perspective of senior managers and the opinions of key stakeholders among others:

Risk appetite must be part of the decision making process. Key questions to ask are:

- A. Are the risks at the right level?** Are the risks and associated consequences understood? – Managed risk taking
- B. Are the risks too high?** Are the mitigations effective? – Recognising our limits
- C. Are we pushing the boundaries enough?** – Identifying opportunities

Risk taking may be desirable because:

- the risks are considered essential to the achievement of aims and objectives
- the risks have the potential to enable realisation of considerable reward/benefit
- the cost of controlling the risks would be greater than the cost of the impact should it materialise
- the risks are clearly understood, communicated and accepted by all affected parties



QUICK GUIDE 4 RISK APPETITE AND TOLERANCE – HOW DO I ASSESS IT? CONTINUED

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	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 undertake 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.

QUICK GUIDE 4 RISK APPETITE AND TOLERANCE – HOW DO I ASSESS IT? CONTINUED

You should engage with key internal and external stakeholders to develop a clear and measurable risk appetite. Decide on the most appropriate areas of risk appetite for your project, programme or area of delivery:

- Do you want to breakdown risk appetite into overarching risk areas e.g. internal, external, strategic and operational?
- Do you want to breakdown risk appetite into sources of risk e.g. political, economic, social, technological etc?
- Do you want to breakdown risk appetite into operational areas e.g. work-stream 1, work-stream 2 and work-stream 3?

This makes sure risk appetite can be separated into manageable sections so that it can be understood and communicated effectively. As risk appetite can vary depending on the project, programme or work-stream it is important to have clarity; to understand and be able to monitor how well risk is being managed. It is useful to have: **Statements**, **Definitions** and **Measures**.

A. **Statements** that set the tone for the appetite for risk. These should be high-level statements that help guide behaviours. A risk statement can help managers and staff take an appropriate level of risk, given the potential for reward. This should focus on the key areas for consideration, whether the focus is strategy, programme and operations; or reputation, finance and people.

EXAMPLE STATEMENT: “We maintain a **cautious risk appetite** towards sustaining appropriate operational processes, systems and controls to support delivery but adopt a **more open appetite** for the development and enhancement of those systems. We are **averse to risks to our statutory objectives and reputation**, however we are prepared to take a stance that may be opposed by some stakeholders where we believe it is necessary to achieve one or more of our key objectives.”

QUICK GUIDE 4 RISK APPETITE AND TOLERANCE – HOW DO I ASSESS IT? CONTINUED

B. **Definitions** that provide lower level examples to clarify meaning for use during day-to-day processes and procedures. This can help guide and advise staff on what is expected of them as part of a programme. For example when staff should **avoid** actions or particular risks, when they should not allow certain things to happen and where people should look to **take more** risk.

C. **Measures** that can actively monitor performance against the appetite definitions as well as the overall statements. This can be taken from appropriate IT and other systems to support the risk management processes, such as financial information, people information, consultation information etc. All forms of measurement need to be appropriate to the relevant environment.

EXAMPLE RISK APPETITE DEFINITIONS	ILLUSTRATIVE MEASURES
Do not disclose sensitive or restricted information	Number of security incidents
Avoid spending or procurement decisions without prior approval	Budget monitoring and forecast information
Take more risk where there is potential benefit to a change in stakeholder engagement	Engagement key performance indicators

QUICK GUIDE 4 RISK APPETITE AND TOLERANCE – HOW DO I ASSESS IT? CONTINUED

We bring the statements, definitions and measures together in the following example:

	RISK APPETITE AREAS				
	FINANCIAL	REPUTATIONAL	TECHNOLOGY	RESOURCES	STAKEHOLDER ENGAGEMENT
STATEMENTS	We are open to taking a Value for Money balance between costs and benefits in delegating financial decision making.	We are averse to any action that could lead to a loss of confidence in the Programme.	We are open to any new or novel digital solutions that might require large scale investment in finance or skills.	We are cautious in how we maintain the appropriate level of leadership for the programme.	We are open to involving all stakeholders in the programme decision making.
DEFINITIONS	Take more flexibility in delegating budgets to appropriate staff below SCS.	Avoid making project decisions without consultation with line management.	Embrace bespoke and innovative technology in all aspects of our delivery.	Do not allow project leads and senior programme positions to fall below appropriate vacancy levels (15%).	Take more steps to engage with stakeholder community on progress and decision points.
MEASURES	Financial monitoring: spend to date and projections.	Programme reports, media exposure.	Programme reports, specialist information technology advice.	HR management information.	Stakeholder responses: quality, quantity and key stakeholder reactions.

NB1: You should exchange the Risk Appetite Areas above for what will be most pertinent to your area, policy or programme – major investment, contract management, environmental impact etc.

NB2: There can be multiple definitions and measures that can support your risk appetite statement if they are needed.

QUICK GUIDE 4 RISK APPETITE AND TOLERANCE – HOW DO I ASSESS IT? CONTINUED

STEP TWO: Implement your risk appetite.

Risk measures can help to identify and monitor risks. Balanced against benefits this can help you achieve your objectives. You need to **communicate** your risk appetite with those who need its guidance to help embed the desired approach. Where risks are high and benefits are low, or benefits are high and risks are low, decision making is easy. The challenge comes when risks and benefits are closely balanced and a risk appetite can help guide decision making.



Risk appetite is established using risk statements, definitions if more detail is needed and measures to monitor your risks effectively. This makes it clearer to people what risk appetite means in practice. Your risk statements can be mapped to a target risk score.

		AVERSE	MINIMAL	CAUTIOUS	OPEN	HUNGRY
EXAMPLE RISK AREAS	Financial					
	Reputational					
	Technology					
	Resources					
	Stakeholders					
		VERY LOW	← TARGET RISK SCORE →			VERY HIGH

NB: The diagram above is an illustration but mapping risk appetite to target risk score can be done for individual risks or using the risk areas you feel are appropriate.

QUICK GUIDE 4 RISK APPETITE AND TOLERANCE – HOW DO I ASSESS IT? CONTINUED

STEP THREE: Monitor and Review your risk appetite.

In monitoring and reviewing your risk appetite you should consider what's working well and what needs to be better:

1. Committing a risk appetite to paper the first time will feel uncomfortable, try to keep it simple and straightforward. Use it, learn from it and review and adjust.

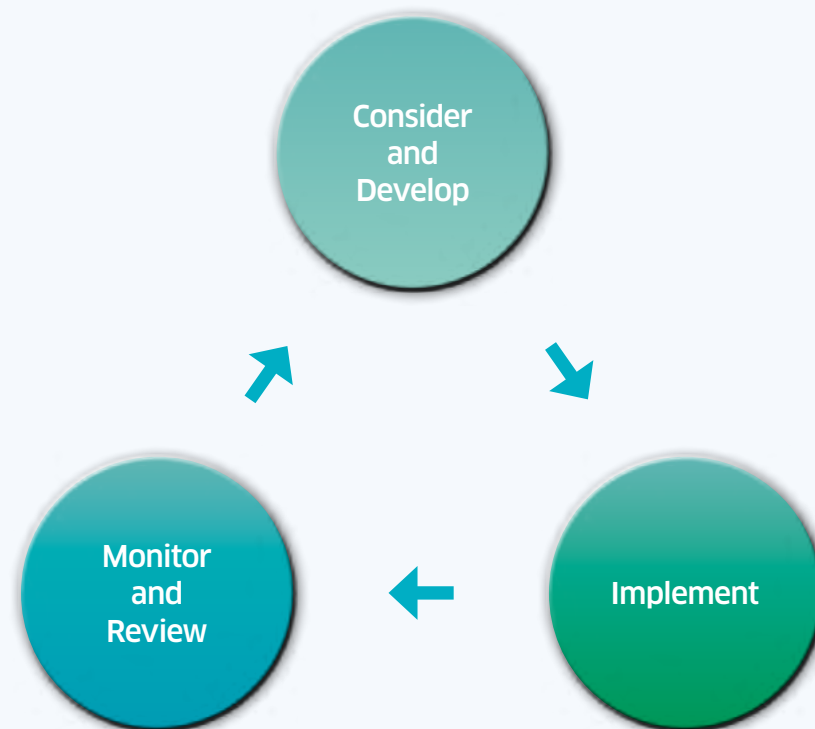
2. Key questions:

- Are you living within your risk appetite?
- Can you live within your risk appetite?
- Why/Why not?

Where you are struggling to live within risk appetite do you:








- need to invest more resource to address? Or
- change your appetite? (e.g. where investment is unaffordable)

3. Risk appetite is about supporting discussions to ensure appropriate risk taking in achieving your objectives. Any approved risk appetite statement (and the definitions and measures that may be used to support it) must be proportionate. Be flexible – you do not need to slavishly apply all aspects of this approach to your project.



QUICK GUIDE 5 PESTLES RISK ASSESSMENT

This table is to provide illustrative examples of the levels of impact a risk may have against the PESTLES categories, your assessment should be data driven and opinion informed.

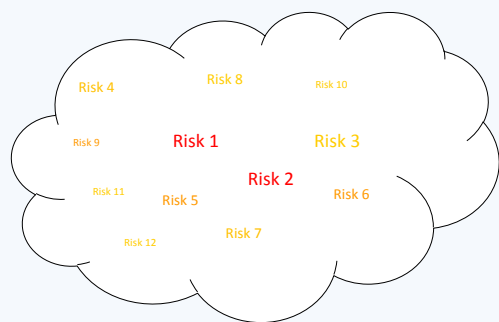
	5 VERY HIGH	4 HIGH	3 MEDIUM	2 LOW	1 VERY LOW
POLITICAL 	Sustained/widespread criticism of a key policy/service, Sustained front page/headline national public criticism lasting at least a week. Events requiring significant time to restore relationships with key stakeholders	Some national public or media criticism lasting at least a week. Events requiring medium length of time to restore relationships with key stakeholders	Widespread local/regional public and/or specialist criticism. Events requiring at least some significant time to restore relationships with key stakeholders	Minor adverse local media coverage. Events requiring 2-3 months to restore relationships with key stakeholders	Minimal issues raised which can be resolved directly with stakeholders has little to no impact on delivery
ECONOMIC 	Impact on budget is unsustainable and will materially impact delivery – up to e.g. 25% of operating budget	Impact on budget is unsustainable and will heavily impact delivery – up to e.g. 20% of operating budget	Impact on budget is sustainable and will have a medium impact on delivery up to e.g. 10% of operating budget	Impact on budget is sustainable with low impact on delivery – up to e.g. 5% of operating budget	Impact on budget is sustainable with low impact on delivery – up to e.g. 1% of operating budget
SOCIAL 	Critical impact on staff for example major disruption caused by industrial action across all locations	Serious impact on staff for example major disruption caused by industrial action across one strategic location	Moderate impact on staff for example moderate disruption caused by industrial action across a number of locations	Minor impact on staff for example minor disruption caused by industrial action across one or more locations	Negligible impact on staff for example minor disruption caused by industrial action in one location
TECHNOLOGICAL 	A critical IT project/system will be delayed by up to one year or never delivered, with substantial financial consequences several customer facing KPIs will be missed.	A key IT project/system will be delayed by up to one year. A customer facing KPI will be missed. A strategic project will be delayed by greater than one year or never delivered.	A key IT system project will be delayed by up to 6 months. An internal KPI will be missed continuously over a period greater than one year	An internal IT system/project milestone will be delayed by greater than one year or never delivered. An internal KPI will be missed continuously over a period of 6 months	An internal milestone will be delayed by less than one year
LEGAL 	A severe breach of regulatory requirements/statutory duties results in enforcement action/sanctions including financial penalties	A major breach of regulatory requirements/statutory duties results in enforcement action including final warning/ compliance activity	A moderate breach of regulatory requirements/ statutory duties results in enforcement action including formal notice/improvement actions	A minor breach of regulatory requirements/statutory duties results in additional action/ formal scrutiny.	An negligible breach of regulatory requirements/statutory duties results in regulatory consequence
ENVIRONMENTAL 	Unforeseen weather event causes severe disruption to frontline service/ delivery of critical government functions with long term ramifications /loss of life.	Unforeseen weather event causes major disruption to delivery of frontline services/key government functions with medium/long term ramifications	Unforeseen weather event causes moderate disruption to delivery of frontline services/key government functions for 1 week.	Localised weather event causes minor disruption to delivery of a frontline service for less than 1 week	Localised weather event causes negligible disruption to services for 24 hours or less.
SECURITY 	Serious unplanned disruption to delivery of public service(s) A front line service suspended for 1+ days. Failure to meet several key customer facing targets Loss of (or security breach to) 0.5% of customer data	Reasonably serious unplanned disruption to delivery of any public service(s). A front line service suspended for up to 1 day. Failure to meet a key customer facing target. Loss or breach of security in relation to <0.5% individual customer records	Any unplanned disruption to delivery of any public service. Failure to meet any customer facing targets	Planned disruption to delivery of any public service. Failure to meet any customer facing targets	Local minor disruption to delivery of any public service.

QUICK GUIDE 6 RISK REPORTING – TOOLS & TECHNIQUES

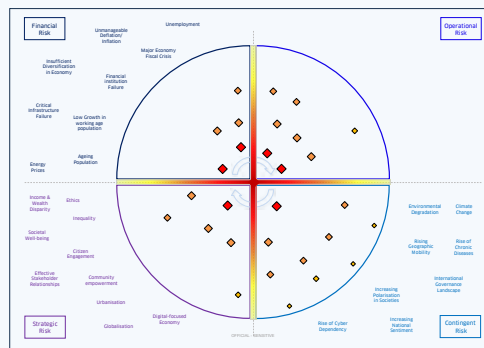
Managing and reporting on your risks doesn't always have to mean just using risk registers to record scores and related information. Utilising this detail and your knowledge of wider outside influences visually can support your understanding of the wider risk landscape and help to recognise current pressures across a project or programme.

Some Examples:

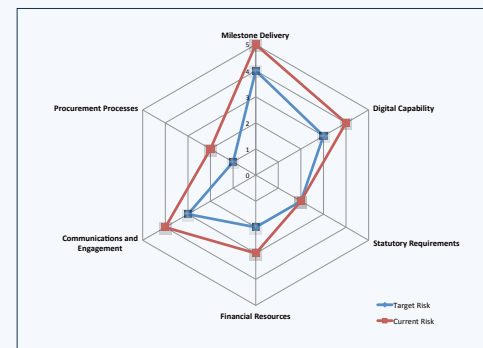
RISK CLOUD



RISK LANDSCAPE



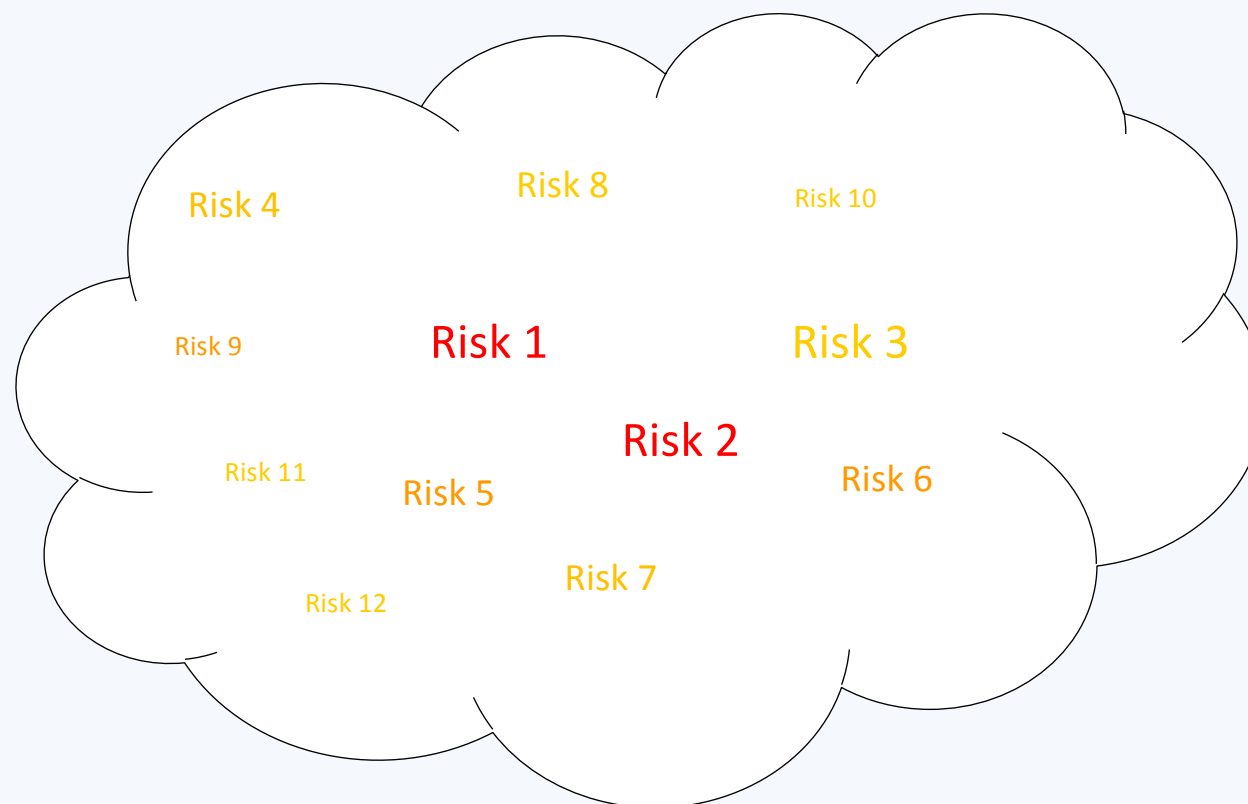
WEB DIAGRAM



For further support on developing your own arrangements you can also contact the Governance and Risk Team.

QUICK GUIDE 6 RISK REPORTING – TOOLS & TECHNIQUES CONTINUED

Risk Cloud

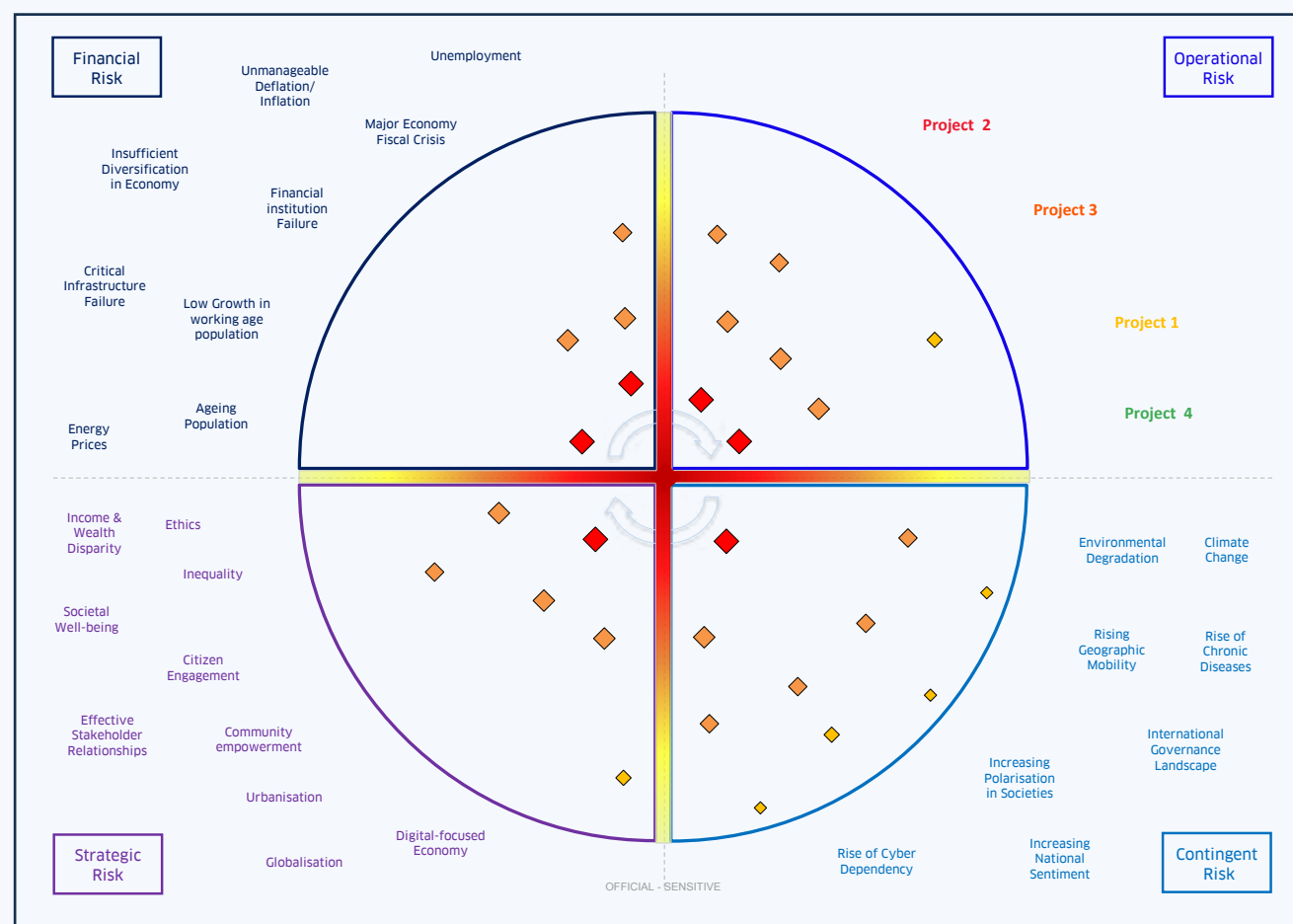


LIKELIHOOD	VERY HIGH	RED
	HIGH	ORANGE
	MEDIUM	GOLD
	RARE/LOW	GREEN

IMPACT	VERY HIGH	28 FONT
	HIGH	22 FONT
	MEDIUM	16 FONT
	RARE/LOW	12 FONT

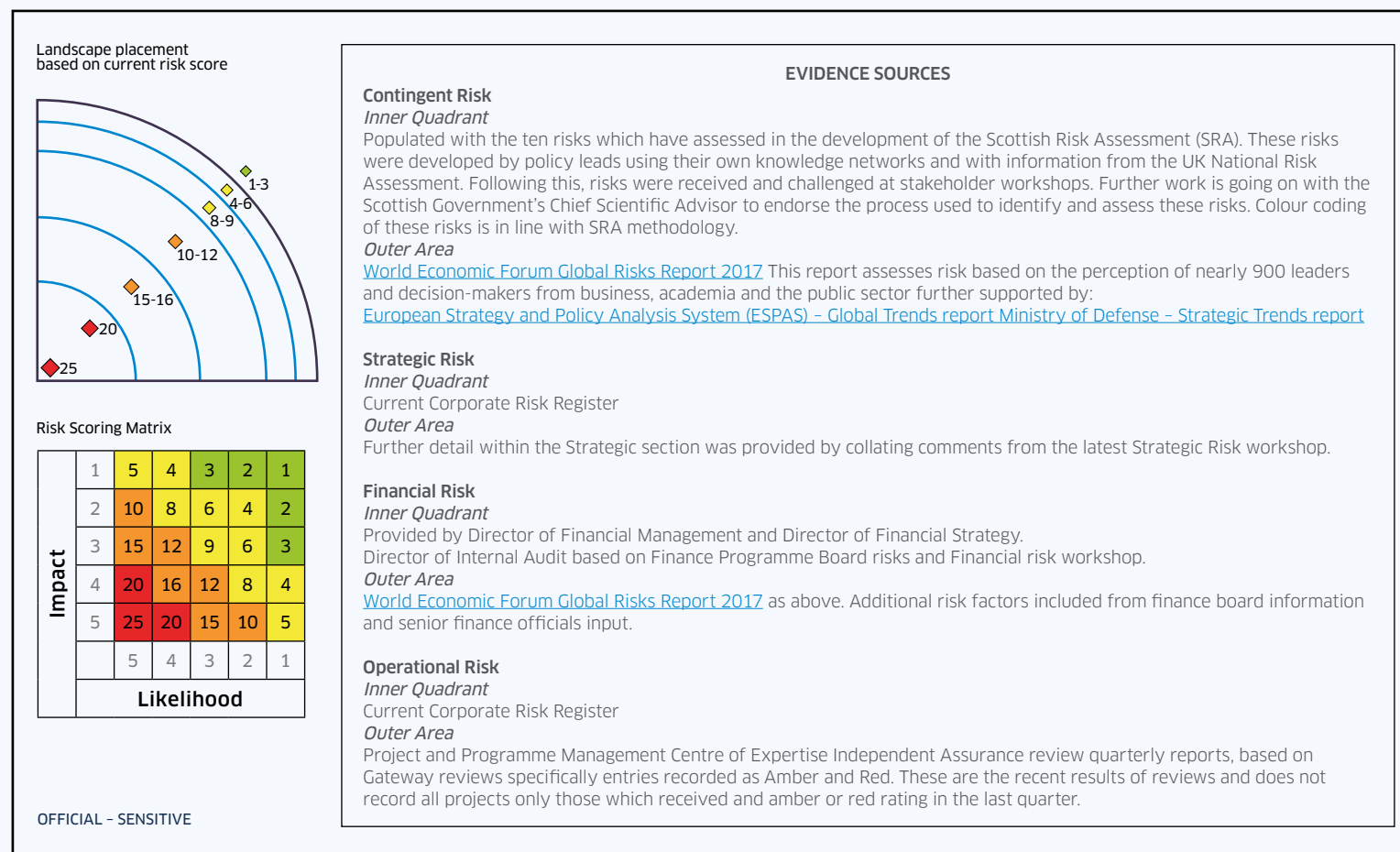
QUICK GUIDE 6 RISK REPORTING – TOOLS & TECHNIQUES CONTINUED

Risk Landscape



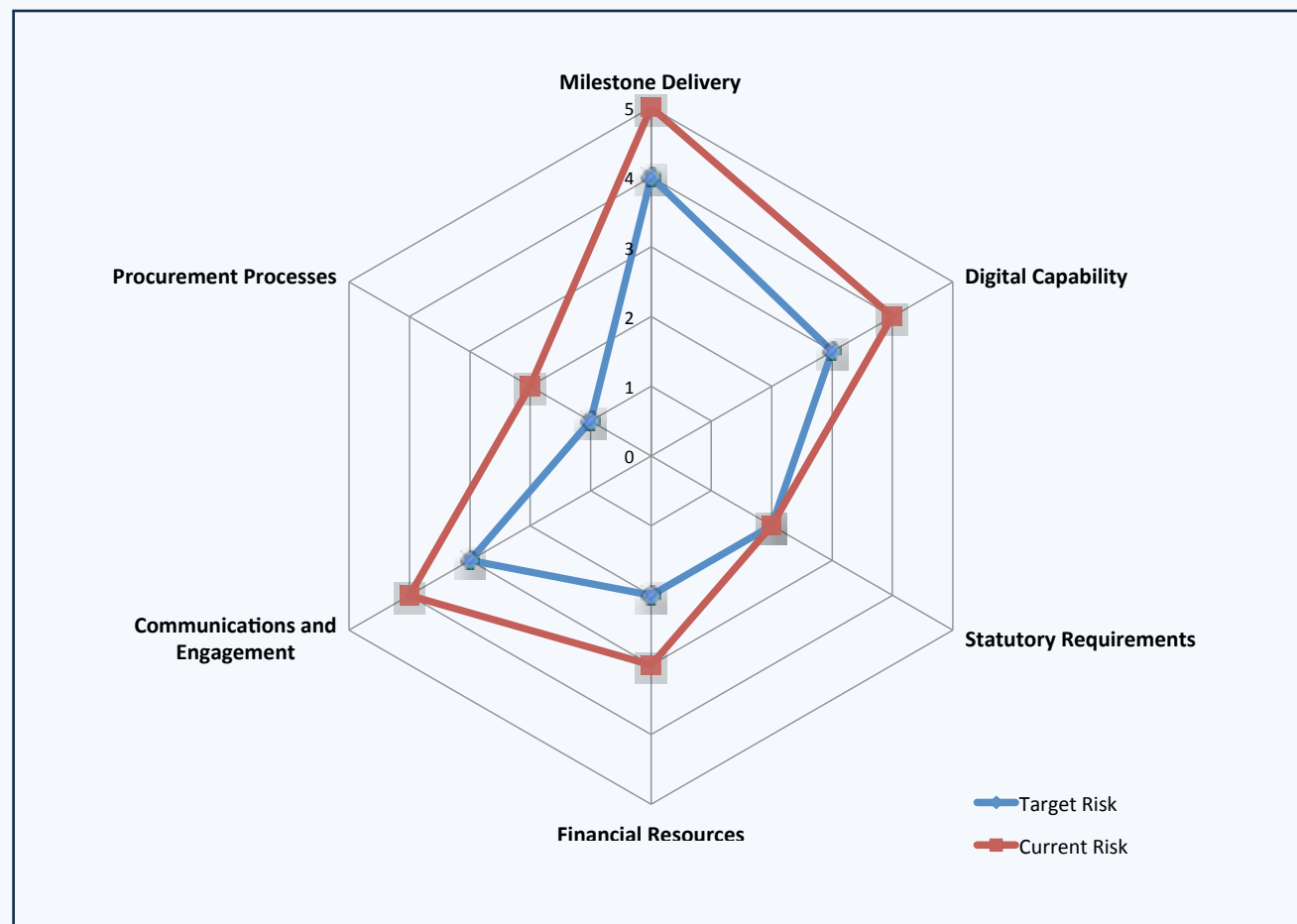
QUICK GUIDE 6 RISK REPORTING – TOOLS & TECHNIQUES CONTINUED

Risk Landscape



QUICK GUIDE 6 RISK REPORTING – TOOLS & TECHNIQUES CONTINUED

Web Diagram



QUICK GUIDE 7 USING THE RISK REGISTER TEMPLATE

The risk register format is based on an internationally recognised risk register model. The content has been kept simple, is in Excel format, uses drop down menus where appropriate (to aid completion) and allows information to be filtered as appropriate 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 ID:

Is a helpful reference and can include links to objectives, outcomes or date initially highlighted (as in the example above). A number reference can aid reporting.

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.

CONTROLS IN PLACE:

This should be a short summary of the key controls in place to manage the risk, to reduce the impact or reduce the likelihood of a risk from occurring e.g. by systems in place or use of specific resources.

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.

QUICK GUIDE 7 USING THE TEMPLATE RISK REGISTER CONTINUED

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 for more detail on what these levels mean see the [Confidence Levels Quick Guide](#).

ACTIONS PLANNED:

This should be a short summary of the key actions planned in order to manage the current risk score. This should be aimed at reducing the risk exposure to the target levels identified in the subsequent columns.

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.

RISK OWNER:

This column is used to identify the most appropriate lead on any given risk. The purpose is not to assign all elements of managing a risk to one person but to ensure there is one point for coordination and reporting purposes.



QUICK GUIDE 8 CONFIDENCE LEVELS – WHAT DO THEY MEAN?

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.

QUICK GUIDE 9 ROLES AND RESPONSIBILITIES



Individuals

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

It is helpful to have a nominated individual(s) from each directorate that have the responsibility to ensure that systems and processes are in place to review and report directorate risks effectively: ensuring risk management information is maintained and communicated. This would also provide a key contact point for DG Business Management Units and the Executive Team Support and Governance Office (ET SGO).



Accountable Officers

Accountable officers (Directors General) are responsible for making sure that effective risk management processes are in place. This includes assuring themselves that effective risk reporting arrangements are established and maintained across all programmes of activity.

To support this each directorate should maintain a risk register and review it regularly. Alongside this the Scottish Government's risk champion, Director General Scottish Exchequer leads on work to provide a support structure for risk management throughout the organisation.



Corporate Board

The Corporate Board is responsible for the risk management strategy of the Scottish Government.



The Audit and Assurance Committee

The Scottish Government Audit and Assurance Committee (SGAAC) is a committee of the Corporate Board is chaired by an Non Executive Director and supports its work by providing assurance that the risk management process is working effectively.



The Governance and Risk Team

Facilitates and supports effective risk management practices throughout the organisation. This includes maintaining guidance and providing training for staff. Bespoke services are also offered including constructive challenge and dedicated workshops. It is the role of individual accountable officers with support from staff to manage risk effectively.

OTHER RESOURCES

The Scottish Government Risk Management approach is supported by the Governance and Risk team that works to:

- develop the Scottish Government risk management framework
- provide advice and guidance on risk management
- deliver training and workshops

For further support email **GovandRisk@gov.scot**

There is also additional guidance available for managing risks in portfolios, programmes and projects available here:

Project and Programme Management Support:

APM Body of knowledge

Government Project Delivery standards

The PPM training framework

Axelos: Prince 2, MSP, M_O_R

Independent Assurance

Further Risk Management Support:

Management of risk in Government – UK Government guidance

Institute of Risk Management

The Orange Book: Risk Management

Other useful resources:

Audit Scotland's Best Value Toolkit

Good Governance Standard for Public Services

Financial Reporting Council: Guidance on Risk Management

© Crown copyright 2017



This publication is licensed under the terms of the Open Government Licence v3.0 except where otherwise stated. To view this licence, visit nationalarchives.gov.uk/doc/open-government-licence/version/3 or write to the Information Policy Team, The National Archives, Kew, London TW9 4DU, or email: psi@nationalarchives.gsi.gov.uk.

Where we have identified any third party copyright information you will need to obtain permission from the copyright holders concerned.

This publication is available at **www.gov.scot**

Any enquiries regarding this publication should be sent to us at
The Scottish Government
St Andrew's House
Edinburgh
EH1 3DG

ISBN: 978-1-78851-409-5 (web only)

Published by The Scottish Government, April 2018

Produced for The Scottish Government by APS Group Scotland, 21 Tennant Street, Edinburgh EH6 5NA
PPDAS274066 (04/18)

w w w . g o v . s c o t