Aberdeen City Council

Risk Management Framework

ABERDEEN
CITY COUNCIL

Shaping
Aberdeen

Aberdeen City Council
Risk Management Framework

Policy Name:	Risk Management Framework
Document No & Review No.	V.1
Policy Type:	Framework Document
Policy Level:	Corporate
Scope:	The Framework applies to all employees and elected members of the Council.
Document Owner	Function: Governance Designation: Chief Officer - Governance
Why do we need this document:	Our Local Code of Corporate Governance (effective 30 April 2017) refers to six principles including: 'Managing risk and performance through robust internal control and strong financial management.' This document sets out the context within which risk is managed at Aberdeen City Council.
Content:	
Appendices:	
Related Policies:	
Date Approved:	
Approved By:	
Review Date:	

CONTENTS

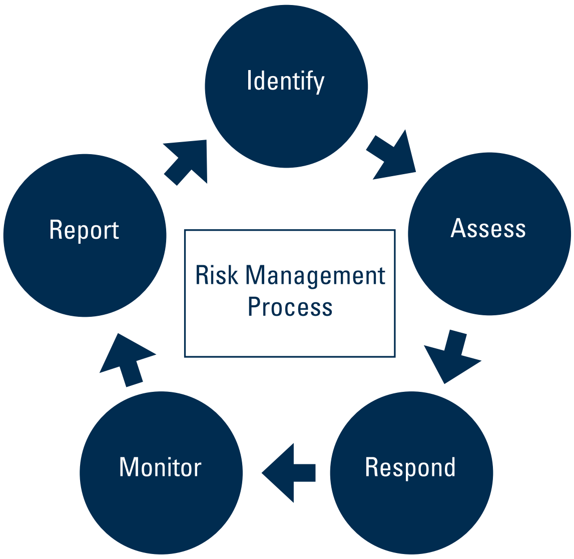
1. Introduction

1.1 Aberdeen City Council is committed to delivering improved outcomes for our citizens and communities through evidenced achievement of our Strategic Priorities. These Priorities are set out in the Local Outcome Improvement Plan 2016-26 and the Strategic Business Plan 2017-18. Our priorities will be achieved through completion of targeted change and improvement activity across the breadth of the Council's functions and services.

1.2 All change and improvement activity comes with some degree of risk. Risk can be defined as the combination of the likelihood of an event occurring and its impact, should it occur. Once risks have been identified, the Council must respond to them in a way which maximises the Council's chances of achieving our corporate objectives.

1.3 Risk management is a tool through which threats to those objectives may be identified, assessed and controlled. This is often referred to as downside risk management. At the same time, we operate in an environment of reducing revenue streams and simultaneously changing demographics and increasing customer-led demand for services. In order to meet these challenges, it may be necessary to take calculated risks and to seize properly risk-assessed opportunities as they arise. Risk management in this context requires actions which maximise benefits whilst simultaneously minimising threats to success. This is referred to as upside risk management.

1.4 The Council's approach to risk management is illustrated by the diagram below:



Risk Appetite

1.5 The appetite for risk is something that people and organisations share. Risk appetite can be seen as a spectrum. At one end, an organisation may be risk averse, that is, they avoid as much risk as possible. Some people and organisations may be found at the other extreme of the spectrum – risk aggressive, actively taking risks in pursuit of benefit. It is the aim of Aberdeen City Council to promote a 'risk aware' culture. The Council should not avoid all risk, nor should it take ill-advised, badly assessed risk. Being risk aware, means that the Council is mindful of both threats and opportunities and by applying risk management methodology, is best placed to deliver the improved outcomes we seek. The Council will consider the development and adoption of a risk appetite statement to support that approach.

2. Risk Management Approach

Risk Management Objectives

2.1 Our framework is based on the following risk management objectives:

- We will promote a risk aware culture throughout the Council which has at its heart, the goal of delivering improved outcomes for communities;
- We will seek to identify, assess and respond to all risks with the potential to undermine the achievement of our Strategic Priorities;
- We will actively identify opportunities with the potential to maximise benefit and ensure that risk management techniques are applied to reduce threat so that opportunities may be managed successfully.

Risk Management Culture

2.2 To promote an effective risk management culture:

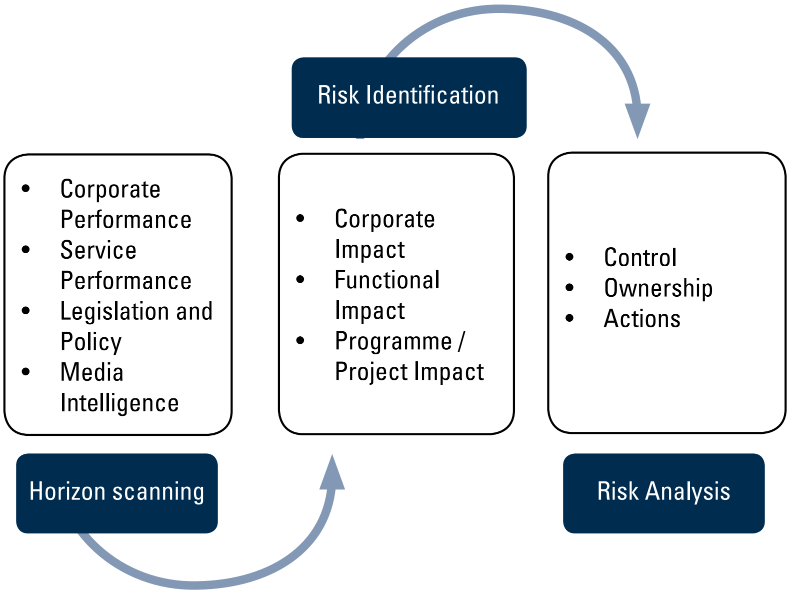
- We will review our Strategic Business Plan annually and ensure it is aligned with the management of corporate risk;
- We will ensure that our corporate risk register is reviewed monthly by the Corporate Management Team, takes account of new and emerging risk through horizon-scanning, the discussion of issues and provides for de-escalation of risks to functional tiers.
- All risk registers will be aligned with business and improvement planning;
- We will ensure risk ownership is assigned to the correct officers to ensure the most effective risk management practices are in place;
- We will provide suitable training to officers to ensure that the necessary skills are in place to facilitate effective risk management;
- We will welcome independent review of our risk management system either by internal or external auditors.

Risk Management Structure

2.3 The risk management structure reflects the tiers of strategic and operational activity where risk may manifest:

- Corporate – risks at this level hold the maximum impact on our ability to deliver our Strategic Priorities and to meet our statutory obligations, with the potential to result in significantly punitive responses by Government and its agencies;
- Functional – risks at this tier affect our ability to deliver efficient and effective services and to meet the expectations of internal and external regulators;
- Programme / Project – risks which if they occur could hamper or terminate the delivery of a one of our major programmes or projects, potentially impacting on the functional or corporate tiers of risk.

2.4 At a general level, risk will be identified and analysed according to the diagram below:

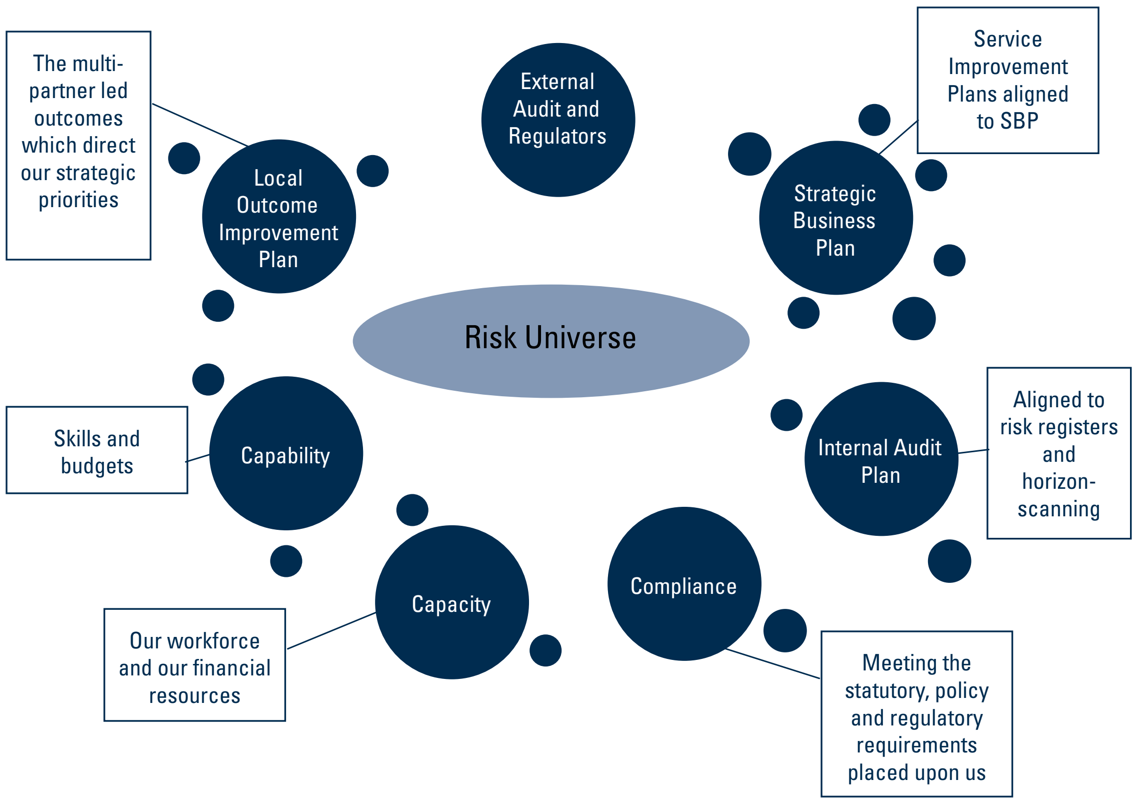


3. Risk Registers

The Risk Universe

3.1 Risk registers are a valuable management tool. A well-constructed register provides for the identification, assessment, monitoring and reporting of risks. They provide managers with key information to support decision-making and the allocation of resources, as well as providing a picture of 'direction of travel' as risks are brought to a tolerable level of control. The risks which are contained within our risk registers are drawn from the Council's 'risk universe.'

3.2 The diagram below summarises the risk universe and the business dependencies which support an effective risk identification process.


The multi-partner led outcomes which direct our strategic priorities
Local Outcome Improvement Plan
External Audit and Regulators
Strategic Business Plan
Service Improvement Plans aligned to SBP
Risk Universe
Skills and budgets
Capability
Internal Audit Plan
Aligned to risk registers and horizon-scanning
Capacity
Compliance
Our workforce and our financial resources
Meeting the statutory, policy and regulatory requirements placed upon us

3.3 The business dependencies identified in the larger circles illustrate the main themes which underpin our risk management methodology. The smaller circles are aligned to these dependencies and will reflect specific issues. For example, capacity will include workforce and resources as its key supporting dependencies, the Strategic Business Plan will be dependent on the Service Improvement Plans and the LOIP draws on Locality Plans.

Risk Registers

Corporate Risk Register

3.4 The Corporate Risk Register (CRR) is owned by the Corporate Management Team (CMT) and reviewed monthly at the CMT (Stewardship) meetings. The risks contained within the CRR reflect the most serious potential impacts facing the Council and these risks are owned and managed by Chief Officers and in some cases, third tier managers.

Functional Risk Registers

3.5 All functions below the corporate tier will require a risk register. Chief Officers will be accountable for risk registers falling within their remit.

Programme / Project Risk Registers

3.6 Programme and Project Managers are responsible for maintaining registers of risks with the potential to impact delivery.

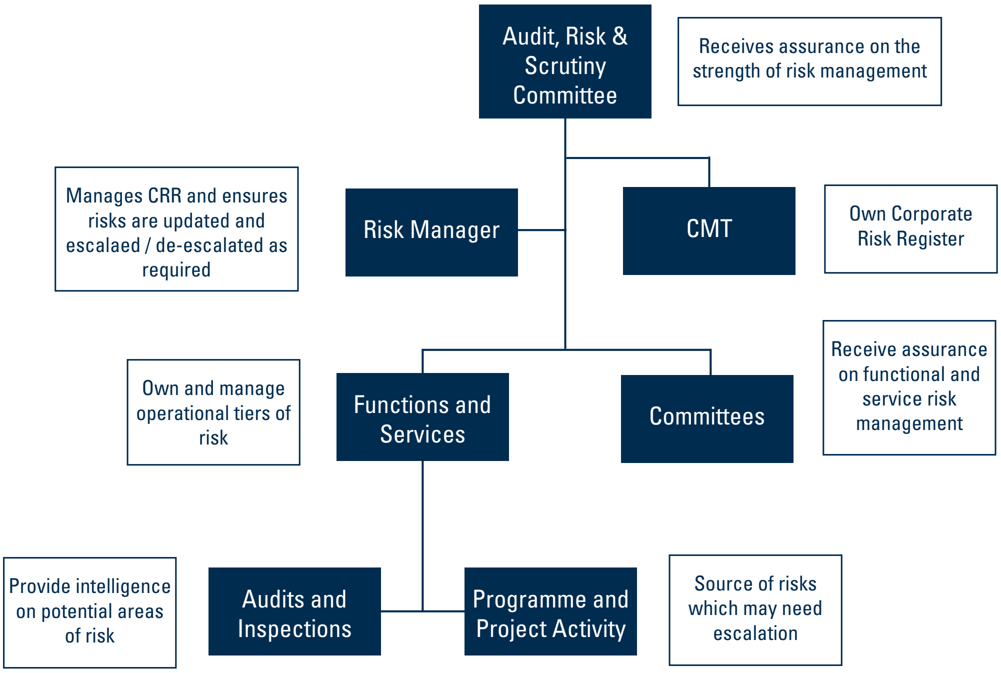
Appendix A provides the format of risk registers.

Responsibilities

3.7 Risk management responsibilities are allocated as follows:

- The Audit, Risk and Scrutiny Committee is responsible for overseeing risk management on behalf of the Council and for receiving assurance that the Corporate Management Team (CMT) are effectively identifying and managing risks with the potential to impact Aberdeen City Council.
- CMT has responsibility for the Council's systems of internal control, which includes the Risk Management Framework and they own the Corporate Risk Register.
- The Risk Manager currently has responsibility for day-to-day management of the Corporate Risk Register, for coordinating risk identification activity and for providing functional and service tiers of operations with training, advice and guidance on risk management matters.
- Committees are currently responsible for receiving assurance on the effectiveness of risk management arrangements in the risk registers falling within their Terms of Reference.
- Management Teams have responsibility for identifying and managing risk in their respective spheres and for alerting the Risk Manager to risks which may need escalation to the corporate tier.
- Programme and Project Managers have responsibility to ensure risks are properly identified and assessed and that risks which are no longer manageable at the programme or project tier, are notified to managers who can determine where escalation is required.
- All members of staff have a responsibility to alert managers to risks with the potential to impact the Council's reputation, finances, infrastructure or the safety and wellbeing of people.

Risk Register Relationships and Responsibilities


Audit, Risk & Scrutiny Committee
Receives assurance on the strength of risk management
Manages CRR and ensures risks are updated and escalaed / de-escalated as required
Risk Manager
CMT
Own Corporate Risk Register
Own and manage operational tiers of risk
Functions and Services
Committees
Receive assurance on functional and service risk management
Provide intelligence on potential areas of risk
Audits and Inspections
Programme and Project Activity
Source of risks which may need escalation

4. Risk Management Process

Risk Identification

4.1 Risks are identified by various methods. For example, the output of activities by external audit, inspectorates and regulatory bodies may reveal areas of risk exposure for the Council in specific functions or in the planning and delivery of essential services.

4.2 Monitoring of performance is another potential source of risk. Spikes in poor performance when properly analysed, may serve to highlight changes to the operating environment or areas where controls are presently inadequate to prevent a risk occurrence. Effective horizon-scanning will serve to further identify impending risks.

4.3 All management teams should periodically conduct an evaluation of threats to the achievement of organisational goals as well as exposure to legal challenge. It is important therefore, that risk is a standing item on the meeting agendas of management, offering not only the opportunity to review the existing risk portfolio but for managers to raise issues which may become risks.

Appendix B details a range of risk identification techniques.

Risk Assessment

4.4 The next stage in the risk management process involves the assessment of risk. This establishes the precise nature of the potential impacts (consequences) of a risk as well as the likelihood of occurrence. Together, these two multipliers provide us with the assessed level of risk. Only when this has been completed can we respond appropriately to a risk. For example, a risk assessed as almost impossible to occur and having negligible impact would in all probability require no action on behalf of the Council and the targeting of resources to a risk such as this would be wasteful and inappropriate. On the other hand, a risk assessed as having a very serious impact and very likely to occur, will require a lot of attention.

4.5 We use a risk matrix to help illustrate the assessment of our risks. This is constructed on a 4 x 6 basis where the 1 - 4 axis reflects impact and the 1 - 6 axis reflects likelihood.

RISK MATRIX

Impact ↓	Score ↓						
Very Serious	4	4	8	12	16	20	24
Serious	3	3	6	9	12	15	18
Material	2	2	4	6	8	10	12
Negligible	1	1	2	3	4	5	6
	Score →	1	2	3	4	5	6
	Likelihood	Almost Impossible	Very Low	Low	Significant	High	Very High

4.6 It is important to reflect on the status of existing controls when assessing risk. Controls serve, when effective, to bring a risk to a tolerable level, usually by reducing the likelihood of a risk occurrence. There are four categories of control:

- Preventive
- Detective
- Directive
- Corrective

4.7 Once controls have been identified, we need to establish their effectiveness. For example, a detective control for a risk around system security, may require frequent analysis of exception and error reports, in order to detect anomalies in the access to our secure systems. If these reports are not routinely analysed, the control is not fully effective. The effectiveness of controls informs the process of risk assessment so that we arrive at a current level of risk and so we can then can target resources at actions designed to make all identified controls effective.

Appendix C details more information on risk assessment.

Business Continuity Plans

4.8 Business Continuity Plans (BCPs) are required for all business critical functions carried out by the Council. BCPs are therefore a key control for corporate and functional risks which relate to the Council's ability to maintain or restore effective operations in these areas following disruption. Corporate and functional risk register reviews should therefore undertake to ensure that emergent risks requiring mitigation by BCPs, are properly identified and recorded. The effectiveness of BCPs as risk controls, is dependent on the frequency of their review and the testing arrangements to which they are subject.

Risk Response

4.9 We categorise our response to risk according to the four 'T's:

- Tolerate. Typically, these would include risks falling within the smallest numerical assessment on the matrix.
- Treat. Most risks which are recorded will be subject to treatment. This will involve the identification and monitoring of actions to increase control effectiveness.
- Transfer. This response typically refers to those risks which carry the highest impact, yet the lowest likelihood of occurrence. Transfer occurs when a third party bears the risk rather than the Council. This is usually through seeking insurance for our assets or when a risk is contractually devolved to a separate body.
- Terminate. This response refers to risks where the impact and likelihood are both at their highest. The causes of the risk, i.e. a project, may be terminated altogether, thereby removing the risk. Alternatively, the project may be re-designed and delivered differently so that the risk becomes less severe and therefore manageable.

More can be found on risk response at Appendix D.

Key Risk Indicators (KRIs)

4.10 All identified controls that are considered to be 'Not Effective' or 'Partially Effective' must have corresponding actions to ensure that the control becomes 'Effective.' Where actions are established to improve control effectiveness, these should be SMART actions. That is:

- Specific
- Measurable
- Assignable
- Realistic
- Time-bound

4.11 By establishing actions on this basis, we can provide an overall assessment of the success of our risk management process against each documented risk. Each action is given a percentage of its completion at each review, normally monthly. The totality of this will provide managers with an indicator showing the success, or otherwise, of activity to control the risk, with a trend chart over time.

4.12 Where KRIs provide intelligence of failing risk management activity, managers may then make informed decisions on where resources should be directed.

Risk Escalation / De-escalation

4.13 Risks need to be managed by the right people, at the right level of management within the Council. Actions required to increase risk control are dependent on the ability of managers to direct resources accordingly. It is the responsibility of risk owners and managers to identify risks which need to be managed at a higher tier, so that a decision can be made whether to propose escalation to a functional or corporate tier.

4.14 Discussions on risk escalation should include:

- New or emerging issues and risks
- Evaluation of new issues and risks
- Decision on the proposed tier where any new risk should lie
- Proposed ownership of the risk
- Any existing controls and mitigation in place

4.15 De-escalation will normally take place from the corporate to functional tiers of risk management. This will be determined by CMT during monthly review of the Corporate Risk Register and will reflect changes in the status of a risk from strategic to operational dependencies.

5. Monitoring, Assurance and Reporting

Risk Monitoring

5.1 Risk management is an ongoing process that needs to be embedded in everyday activity. The process must be reviewed on a regular basis to remain effective. This framework will be subject to annual review to ensure continued effectiveness and that it takes account of the wider operating environment.

5.2 It is the responsibility of each risk owner and manager to review risks on a regular basis and identify whether any revisions are required. The revision may involve a re-assessment of the risk by impact and likelihood or planned mitigating actions, or simply an update in the notes column.

5.3 On a quarterly basis, each Chief Officer will seek assurance from functional tiers within their remit, that risks are being adequately monitored and actions are being completed as agreed in formal action plans.

Control Action Plans

5.4 Risks identified for ‘treatment’ will require action plans to bring identified controls to full effectiveness. Each action detailed in the control action plan should:

- Provide a title for the action;
- Describe the nature of the action and the impact its completion will have;
- Indicate by a percentage, the extent of the action’s progress toward completion;
- Detail the due date for completion and any revised due date, should slippage occur;
- Provide an update giving context around the status of the action; and
- Identify the action’s owner.

Appendix A provides information on the style of control action plans.

Reporting and Assurance

5.5 Risk assurance is an essential component of the risk management framework. Assurance is required so that managers and elected members can have confidence that the approach to managing risk is successful.

5.6 Risk assurance maps for our medium and long term risks detail the sources of internal and external assurance for each specific risk and grade the quality of the assurance source as red, amber or green. For example, a recent audit report or intelligence received from an external regulatory body would be graded as green, reflecting the quality of the assurance we may take from it. Older sources of assurance may be less valuable and in cases where an assurance source is known but no or little activity has taken place for some time, the status would be red. In this way, assurance 'gaps' may be identified and resources targeted accordingly.

5.7 Assurance maps are a valuable tool for medium and longer term risks where a continual 'watching brief' needs to be maintained. Assurance maps are not usually relevant to short-term risks reflecting specific programmes or projects.

Appendix E details an example assurance map.

5.8 Other methods of providing assurance are in place through the design of risk registers. These allow decisions to be made whether:

- The risk is properly identified through its title and definition;
- The controls are correct and their relative effectiveness is properly established;
- The current risk assessment properly reflects the status of controls;
- The correct risk owner and day-to-day risk manager have been identified;
- Control actions are in place to support control effectiveness.

Risk Reporting Structure

5.9 The Corporate Risk Register and Action Plan will be reviewed by the Corporate Management Team (Stewardship) monthly and will be presented as part of an annual risk management assurance report, to the Audit, Risk and Scrutiny Committee.

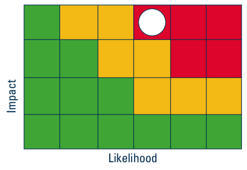
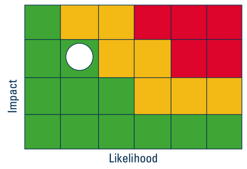
5.10 Other risk registers and their associated action plans will be subject to review by directors and their management teams at least quarterly. Committees will oversee registers reflecting risks falling within their Terms of Reference, as well as receiving an annual report on effectiveness and forward plan scheduling.

5.11 The Audit, Risk and Scrutiny Committee will receive all risk registers annually.

Appendices

Appendix A

Risk Register Template

Code		Risk that			
Definition					
Potential Impact		Causes	Control Effectiveness		Current Risk Assessment
			Control	Control Assessment	
					
					Very serious
					Significant
Risk Owner			Risk Manager		Residual Risk Assessment
Latest Note					
					Serious
					Very Low

Control Actions

Action	Progress	Original Due Date	Amended Due Date
	0%		
Description			
Update			
Assigned To			

Appendix B

Risk Identification Techniques – Advantages and Disadvantages

Technique	Advantages	Disadvantages
Questionnaires and checklists Structured questionnaires and checklists aimed at deep diving into priorities, processes and dependencies to identify areas of risk.	Consistency of approach and consistency of output. Involvement of a broad range of management tiers possible.	May be too rigid and inhibit dynamism. No opportunity for interaction with peers. Questions posed will tend to be based on history alone.
Workshops and Brainstorming Sharing ideas to discuss the events which could impact priorities, processes and dependencies. (Often use a PESTLE or SWOT approach)	Consolidated opinions from parties leading to a consensus driven output. Face to face debate and interaction is a dynamic approach.	Senior managers tend to dominate. Right people may not be invited or may not attend.
Inspections and Audits Inspections of premises and activities and compliance and control audits of established systems and procedures.	Physical evidence drives opinions. Audit approach usually well-structured.	Audits tend to focus on historical events (reactive) and miss emerging risks in the wider environment. Inspections may be narrowly focused.
Dependency Analysis Analysis of the processes and operations within the organisation to identify critical components and their exposure to risk.	Leads to improved understanding of processes with a greater likelihood that no critical functions will be missed.	May not be suitable for strategic level risk identification. Can be time-consuming and resource intensive.
Delphi Technique Consulting a range of experts with expertise in various aspects of the project for their views on risk. Questionnaires are designed by a 'staff group' and issued to experts. Results are collated and analysed in an attempt to achieve consensus.	Experts will have the required level of knowledge and understanding of key dependencies and processes.	Can be time-consuming and expensive. Experts may overstate risks in their own areas of expertise.

Scenario Analysis Process of analysing possible future events by considering alternative possible outcomes so instead of one exact picture of the future, typically, 3 alternative scenarios are presented: an optimistic, pessimistic and most likely scenario.	Avoids reliance on the past and knowledge of historic events. Provokes discussion with the aim of reaching consensus.	Can rely on significant degree of subjectivity and may ignore some factual data.
Systems Dynamics Often used in change management situations. Focuses on interrelationships between component parts of the business and their influence on the effectiveness of the total process.	Useful in organisations where there are strongly differentiated functions such as HR, IT, Finance etc. but which are at the same time interdependent.	Requires significant expertise in understanding the interrelationships between planned activities or potential risk events.

Appendix C

Risk Assessment

The following details the steps to be taken when applying an assessment rating (score) to an identified risk. The Council implements a 4 x 6 risk matrix to reflect assessed level of risk, where the 4 scale represents the impact of a risk and the 6 scale represents likelihood of a risk event occurring.

Impact

The first step is to examine the potential impacts which have been identified. The severity of these impacts will determine where the risk will sit on the 1-4 scale. The potential impacts of the risk will be determined by applying criteria, as in the example below:

Negligible	1	Managed incident, almost no people, economic (financial), social, technological, legal, environmental impact.
Material	2	Local media interest, customer complaints, significant disruption
Serious	3	National media interest, negative reputational impact, serious loss of confidence and Government censure, prosecution / litigation
Very Serious	4	Major national media interest, death or injury, prosecution / litigation, public outcry, special measures

Likelihood

The likelihood of a risk event occurring determines where the risk is placed on the 1-6 scale. The table below provides examples of how to apply this placing.

Almost Impossible	1	Once in 50 years
Very Low	2	Once in 20 years
Low	3	Once in 10 years
Significant	4	Once in 5 years
High	5	Once in 1 year
Very High	6	Once in 3 months

Using this methodology will lead to a baseline risk assessment.

Control Effectiveness

The risk assessment arrived at using the approach detailed above will now need to take account of the controls which must be identified for every risk. Controls will broadly fall within one of the following four categories:

Category	Control Examples
Preventive	Segregation of duties (e.g. authorisers and requisitioners under the Procurement Regulations); access controls to confidential systems
Detective	Exception reports; reconciliation processes; error reports
Directive	Accounting manuals; documented procedures (e.g. Following the Public Pound); Scheme of Governance (including delegated powers, Financial and Procurement Regulations); training; management supervision and oversight
Corrective	Complaint handling; virus isolation; incident resolution

Once controls have been identified, an analysis of their effectiveness has to be made. Controls may be 'Not Effective', 'Partially Effective' or 'Fully Effective.' The ultimate goal of risk management is to ensure all identified controls reach a state of Full Effectiveness.

For example, we have identified a risk around health and safety. One of the controls is that all managers at a particular level have received appropriate training in managing health and safety incidents. The Organisational Development Team have advised that currently, 50% of the managers requiring the training have received it. This control is therefore partially effective.

For all controls which are not effective or partially effective, there should be a corresponding action to improve effectiveness. In the case of the example above, the action would be to ensure all appropriate managers receive the training. The current progress status of the action would state '50%.' As further training is delivered, the progress would increase until eventually the action is complete. The control would then become fully effective.

In most cases, controls reduce the likelihood of a risk event occurring. The control that managers will be trained in health and safety incidents reduces the likelihood of a risk that an incident is not properly handled. It does not reduce the impact of the incident on the individual or individuals caught up in the incident. So the effect of the control is to move the likelihood down the 1-6 scale.

In a minority of cases, controls may serve to reduce the impact of a risk event. For example, we have identified a risk that the Council loses access to part of the core office accommodation through fire, flood or structural damage. We reduce the likelihood of a risk event as far as possible through implementing controls such as fire risk assessments, structural surveys, regular testing of safety systems etc. The impact of a risk event of this kind would be very serious. Essential services may not be delivered, vulnerable groups may be placed at risk. We apply key controls which include Emergency Planning and Business Continuity Plans. These ensure that staff may be alerted to work from home where possible; that alternative premises are rapidly made available; that we seek support from partner organisations. These controls can mitigate the impact of the risk event on the community.

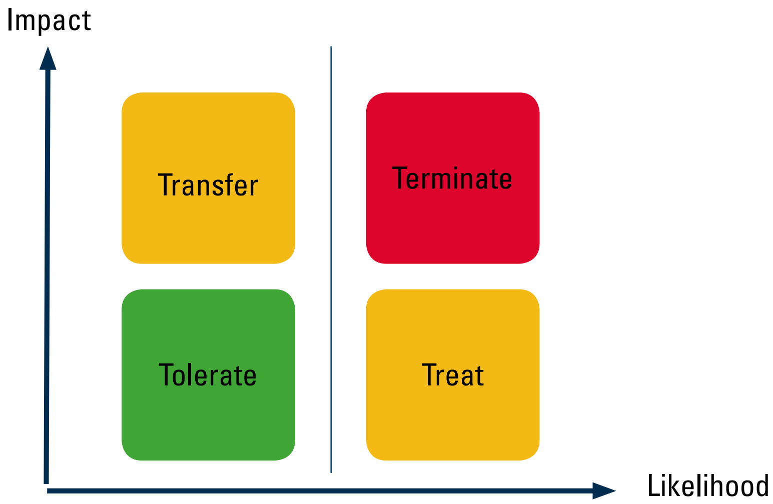
The relative effectiveness of the controls will determine the current risk assessment. Where the majority of the controls are not effective, the risk assessment will be at or close to the baseline assessment and will fall within the red area of the matrix. Where most of the controls are partially effective, the risk will probably fall within the amber area of the matrix. Where controls are mostly fully effective, the risk will be expected to fall within the green area.

The movement of a risk through the matrix over time, as control effectiveness improves, is an important management tool providing assurance that risk management approaches are successful.

Appendix D

Responding to Risk

Risk Response reflects how we approach the risks we have identified and assessed. The 4 'Ts' describe this approach. The diagram provides a simple illustration of the nature of response typically required for assessed risks.



Tolerate

Risks which have reached a level where it is considered acceptable for the Council to bear and where further efforts to mitigate the risk would not be cost effective in terms of achieving additional benefit to the business, will fall into this approach. Where risks are assessed as tolerable, they may be removed from risk registers. For project level risk, it is beneficial however to retain all identified risks regardless of their level in the project risk register. Typically, tolerable risks will be assessed as low likelihood and low impact and occur in the 'green' area of the heat map.

Treat

In this response, active measures to control and mitigate the risk have to be taken. These measures may be to reduce the likelihood of a risk event, or to reduce the impact on the Council and its business if an event were to occur.

It is important to actively monitor risks identified for treatment and ensure a regular re-assessment regime is in place so that progress towards an acceptable level of control or 'tolerability' is evidenced. The level of assessed risk in the heat map will determine the frequency of review.

Transfer

Sometimes, it is not cost-effective or practical for the Council to manage all known risks. Transfer has traditionally meant insurance in the public sector. By obtaining insurance cover for a service or function such as motor liability, employer liability or public liability, we transfer the burden of risk control to a third party. In more recent times, the growth of arms-length external organisations (ALEOS) has meant that some risks are transferred to third parties through contractual arrangements. These include service level agreements (SLAs) with providers. It is worth bearing in mind that a risk can never be wholly transferred, there will always be some residual risk to the Council. For example, an increase in motor liability claims could lead to media coverage and reputational damage to the Council. The increase in partnership working, for example the integration of health and social care, also has implications for risk management with some risk transferred to a partner organisation, and other risk transferred to the Council.

Terminate

Where a risk is high impact and high likelihood in our assessment, the model above suggests we should terminate it. This means in effect, terminating the causes of the risk. This is commonly adopted in the commercial sector where for example, negative customer feedback about a new product or higher than anticipated production costs and lower than predicted market share, may prompt the termination of the production and therefore the risk.

In the public sector this is less straightforward. Often, there are statutory responsibilities in service provision to fulfil and termination of the source of a risk may not be an option. Where, however, we have developed innovative methods of service delivery and these prove to be riskier than first predicted as projects unroll, there may come a point where termination to reduce loss, harm to individuals and communities or reputational damage becomes imperative and the project or work stream is ended. In the model above, these risks are identified as red, the riskiest area of the matrix.

Positive or ‘Up-side’ Risk

Risk management is not solely concerned with reducing the level of threats to an organisation’s business. The commercial sector has always taken calculated risks in order to further their business objectives. Increasingly, the public sector is looking at innovative methods of service delivery in order to meet the challenges of increasing demand, demographic change and decreasing revenue.

In positive risk management, or opportunity risk, instead of implementing measures to reduce the likelihood and impact of risk materialising, measures are required to increase likelihood and to enhance impacts.   In this sense, there is a fifth ‘T’ – ‘Take the Opportunity.’

Appendix E

Assurance Maps

Assurance mapping is a tool which serves to identify the full range of sources of assurance to an identified risk in order to provide managers with a picture of the relative strength of those assurances. In the template below, the categories of assurance in the top row do not change, regardless of the risk concerned. The assurance sources however, will vary from risk to risk. These may include reports of audits or inspections, documented procedures and policies and regular management consideration of controls.

Applying red, amber or green to the assurance source details its relative strength.

Assurance Source	Frequency	Internal sources of assurance				External sources of assurance				Assurance conclusion	Lead Officer
		Policy & procedural Notes	Compliance	Management Control and Review	Risk Management	Third Party Report	Legal	Internal Audit	External Audit		

Inadequate Assurance	Moderate Assurance	Strong Assurance

ABERDEEN
CITY COUNCIL

Shaping
Aberdeen

DSC0794 - BR/RMF/05/02/2018