GLASGOW CITY COUNCIL

RISK MANAGEMENT POLICY AND FRAMEWORK

Policy Statement and guidance and templates for risk management

April 2018

GLASGOW CITY COUNCIL
RISK MANAGEMENT POLICY AND FRAMEWORK
CONTENTS

Section	Title	Page
1	**RISK MANAGEMENT POLICY STATEMENT**	1
1.1	Introduction	1
1.2	Risk Management Policy Statement	1
1.3	Applicability	2
1.4	Governance	2
2	**RISK MANAGEMENT FRAMEWORK**	3
2.1	Introduction	3
2.2	Risk Management Process and Lifecycle	5
3	**RM PROCESS STAGE 1: IDENTIFY AND RECORD RISKS**	6
3.1	Risk Identification	6
3.2	Importance of Objectives	6
3.3	Risk Identification Techniques	6
3.4	Risk Categories	7
3.5	Describing Risks	7
3.6	Bow Tie Analysis	8
3.7	Recording Risks – Risk Register	8
4	**RM PROCESS STAGE 2: ANALYSE AND ASSESS RISKS**	10
4.1	Risk Analysis and Assessment	10
4.2	Assessing Probability	11
4.3	Assessing Impact	11
5	**RM PROCESS STAGE 3: RESPOND TO RISKS**	13
5.1	Responding to Assessed Risk Scores	13
5.2	Risk Appetite and Tolerance	14
5.3	Management of Risks	14
5.4	Identification of Risk Owners and Responsible Officers	15
5.5	Treating Risks with Control and Mitigating Actions	16
5.6	Risk as Opportunity	17
6	**RM PROCESS STAGE 4: MONITOR AND REPORT**	18
6.1	Monitoring Risks	18
6.2	Escalating and Reporting Risks	19
6.3	Review – Points for Consideration	20
6.4	Summary of Risk Reporting	21
7	**RM PROCESS STAGE 5: INTEGRATE**	22
7.1	Integration of Risk Management	22
8	**ROLES AND RESPONSIBILITIES**	23
8.1	Elected Members	23
8.2	Chief Executive	23
8.3	Extended / Corporate Management Team	23
8.4	Director of Governance an Solicitor to the Council	23
8.5	Service Directors	24
8.6	Service Leadership / Senior Management Teams	24
8.7	Head of Audit and Inspection	24
8.8	Corporate Governance	24

GLASGOW CITY COUNCIL
RISK MANAGEMENT POLICY AND FRAMEWORK
CONTENTS (cont.)

Section	Title	Page
8.9	Service Managers	25
8.10	Risk Owners	25
8.11	Financial Services Insurance Section	25
8.12	Employees	25
8.13	Service Risk Champions	26
8.14	Operational Risk Management Forum	26
9	**GOVERNANCE AND COMPLIANCE**	27
9.1	Internal Audit	27
9.2	Links to Business Continuity	27
9.3	Best Value	27
10	**DOCUMENTATION AND RECORDS MANAGEMENT**	28

Appendix	Title
1	Risk Register Template and Guidance Notes

VERSION CONTROL

Document Owner: Laura Heggie, Tel: 0141 287 3771, email: laura.heggie@glasgow.gov.uk

Effective Date: 30 April 2018

Date	Version	Author	Approved By	Comments
January 2018	V0.1	Laura Heggie	N/A	Initial draft issued to risk community for review
March 2018	V0.2	Laura Heggie	N/A	Updated to reflect feedback from risk community, notably the risk assessment matrix at section 4 Issued to C Forrest for approval
April 2018	V1.0	Laura Heggie	Carole Forrest, Director of Governance and Solicitor to the Council	Final version published on 30 April 2018

SECTION 1 RISK MANAGEMENT POLICY STATEMENT

1.1 INTRODUCTION

1.1.1 This document consists of a Policy Statement, which outlines the Council's approach to Risk Management (RM), and an operational Framework which explains the processes, activities and roles and responsibilities required to successfully implement the Policy.

1.2 RISK MANAGEMENT POLICY STATEMENT

1.2.1 Glasgow City Council (the Council) is aware that a certain level of risk can never be eliminated and is wholly committed to the pro-active identification and management of risks within its control.

1.2.2 This Policy Statement sets out why and how this will be done and is the foundation for the detailed RM Framework which provides guidance and tools to be implemented across the Council.

1.2.3 The objectives of the RM Framework are to:

- raise the profile and embed a RM culture across all Council Services, making it a core part of strategic planning, decision making, programme and project management, business continuity and Health and Safety;
- deliver a consistent approach to RM across all Council Services;
- promote an inclusive approach to RM across the Council and encourage ownership of the RM process and specific risks;
- raise awareness of risks across the Council and inform staff of their responsibilities in relation to, and the importance of, RM;
- allow continuous improvement and increased resilience through anticipating and responding to risks, both as potential threats and opportunities and linking to business continuity planning;
- preserve and enhance service delivery; reduce injury, loss and damage to assets; safeguard employees, and maintain effective stewardship of public funds, and
- protect the integrity of the Council's services; its corporate governance framework and its reputation.

1.2.4 The Council recognises the importance of RM and the requirements it places on staff across the organisation. The successful implementation of this Policy requires:

- Ownership by, and commitment from, the Extended Council Management Team (ECMT).

- The nomination, by Directors, of named officers to represent their Service and to manage operational compliance with this Policy and the implementation of the RM Framework.

- The engagement of these nominated officers with the Council's Operational Risk Management Forum (ORMF) to ensure consistency in the implementation of this Policy and the RM Framework and to share experience and best practice.

- The commitment of Executive Directors and Service Senior Management Teams to embedding the RM Framework in their management and operational structures and to ensure compliance with all aspects of this Policy and the RM Framework, including ensuring that:
    - appropriate resources are allocated to implementation;

- risks are identified, recorded in Risk Registers and regularly reviewed, escalated as required, and reported to appropriate governance structures, and
- control and mitigating actions are identified, resourced and implemented to manage risk to an acceptable level.

1.3 APPLICABILITY

1.3.1 This Policy applies to all Council Services and all sections/functions/teams therein and all are required to apply this methodology.

1.3.2 Across the wider Council Family, ALEOs may have their own policy and arrangements for risk management. However, they are strongly encouraged to adopt this Policy and Framework to ensure consistency of approach.

1.4 GOVERNANCE

1.4.1 This Policy and Framework will be governed by Corporate Governance, reporting to the Director of Governance and Solicitor to the Council, who has responsibility for risk management.

1.4.2 Regular reports on the performance of the Framework will be provided to the appropriate Council Committee.

1.4.3 This Policy and Framework are aligned to best practice principles from HM Treasury Orange Book[1], ISO31000:2009 and the Association of Local Authority Risk Management (ALARM)[2] guidance.

1.4.4 This Policy and Framework will be subject to regular review.

Further information can be obtained from: corporategovernance@glasgow.gov.uk

Or on Connect at
http://connect.glasgow.gov.uk/article/22018/Risk-Management

1 https://www.gov.uk/government/publications/orange-book
2 https://www.alarm-uk.org/

SECTION 2 RISK MANAGEMENT FRAMEWORK

2.1 INTRODUCTION

What is Risk?

2.1.1 Risk is related to uncertainty and is defined as the "effect of uncertainty on objectives"[3]. The presence of uncertainty means that the outcomes of events and actions can only be estimated however, as well as presenting potentially negative threats, risk can also present positive opportunities.

2.1.2 Risk is the chance an action or event may happen that could have an impact on the Council's ability to achieve its objectives. Risk is a deviation from what is expected and it is the combination of the probability of an action or event happening i.e. something that may, or may not, happen, and the impact or consequences that could arise if it were to happen. The concept of probability and impact is detailed in section 4.

What is Risk Management?

2.1.3 Risk management (RM) is defined as "coordinated activities to direct and control an organisation with regard to risk. The culture, processes and structures that are directed towards the effective management of potential opportunities and threats to the organisation achieving its objectives."[4]

2.1.4 It is a proactive process and a central part of the Council's corporate governance framework. The objective of RM is to identify and assess risks and plan and implement the actions that are required to avoid, mitigate or manage, as far as possible, the impact of the risk occurring and keep this under review.

2.1.5 Risk management is undertaken at all levels across the Council including (i) strategic level; (ii) Service level; (iii) Service-area / team / function level, and (iv) programme and project level. However it is crucial that all levels are integrated and support and inform one another.

2.1.6 Wherever there are objectives or planned outcomes, there will be a need for risk management. However, it is recognised that risk management arrangements must be proportionate as over-engineering can potentially stifle innovation and change.

2.1.7 Increasingly, effective RM is important where there is increasing financial pressure on the Council and as service delivery models and technology change.

Applicability of the RM Framework

2.1.8 This Framework has been endorsed by the Council's Corporate Management Team and is applicable, wholly and entirely, to all Council Services.

[3] ISO31000:2009
[4] ISO31000:2009

2.1.9 Its application is mandatory and implementation and adherence will be monitored by Corporate Governance, reporting to the Director of Governance and Solicitor to the Council, who has responsibility for RM.

2.1.10 The approach and associated documentation is advocated for use by the Council's Arms' Length External Organisations (ALEOs). It is recognised that the ALEOs are responsible for the design and implementation of their own RM arrangements however the adoption of this Framework is strongly recommended.

2.1.11 Corporate Governance is responsible for undertaking regular reviews of the Framework to ensure it remains fit for purpose.

Benefits of RM

2.1.12 Risk will never be eliminated therefore a robust approach to RM is required which will deliver the following benefits:

- Improved efficiency of operations and service delivery;
- Demonstration of good governance;
- Support the attainment of objectives;
- Better delivery of intended outcomes;
- Improved and informed decision making and resource allocation;
- Increased accountability for, and mitigation of, identified risks;
- Increased ability to secure funding;
- Maximisation of opportunities and supports innovation;
- Protection of reputation;
- Protection of budgets from unexpected financial losses;
- Protection of assets;
- Improved organisational resilience to risk;
- Compliance with legislation including the Civil Contingencies Act, Health and Safety etc. and emerging and evolving best practice;
- Enables efficient pro-active planning and reduces the need to react to risk i.e. less 'fire-fighting', and
- Increased awareness of risk.

Structure of the Framework

2.1.14 The Council's RM Framework is comprised of the following elements, each of which will be considered in detail throughout this document:

(i) **Risk Management Process and Lifecycle**:

a. Identify and record risks
b. Analysis and assessment of risks
c. Respond to risks
d. Monitor and report
e. Integrate with strategic planning and decision making

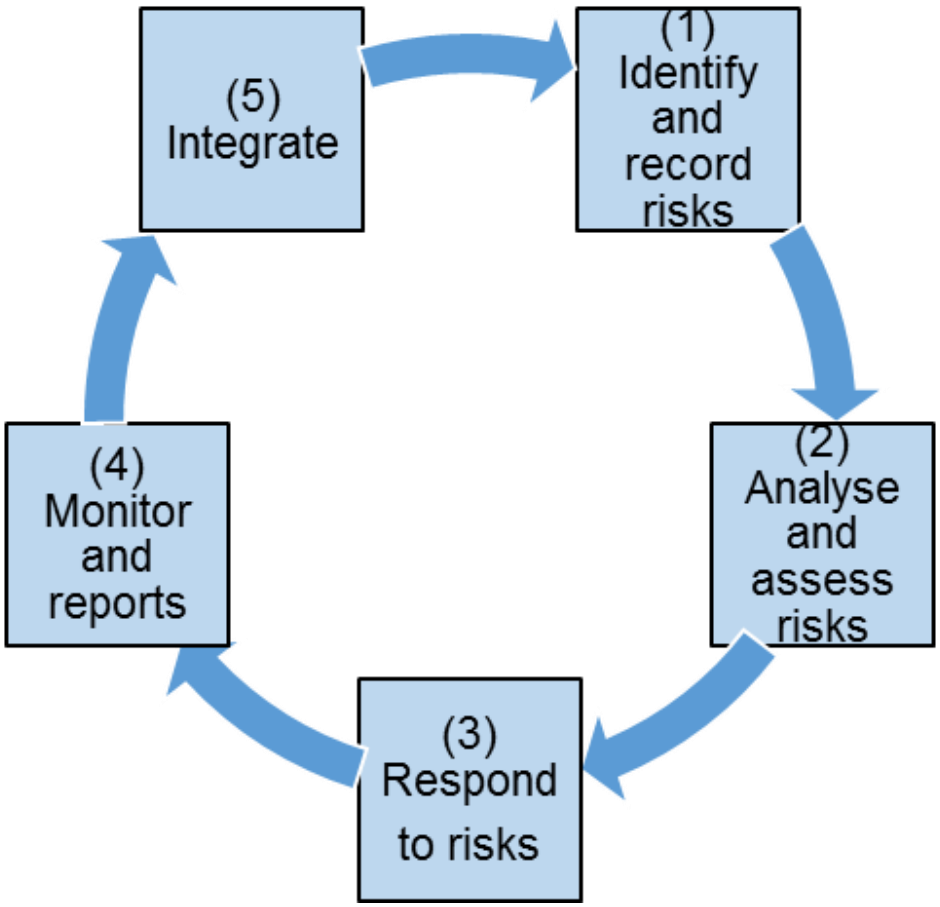
(ii) **Roles and Responsibilities**

(iii) **Governance and Compliance**

2.2 RISK MANAGEMENT PROCESS AND LIFECYCLE

2.2.1 The theoretical RM lifecycle is outlined in Illustration 1 below. This has been used as the basis for the Framework, in accordance with recognised best practice set out by the set out by Association of Local Authority Risk Managers (ALARM)[5].

Illustration 1: Risk Management Process



[5] https://www.alarm-uk.org/

SECTION 3 RM STAGE 1: IDENTIFY AND RECORD RISKS

3.1 RISK IDENTIFICATION

3.1.1 Risk identification involves considering what might happen, within and out with the Council, which could have an effect on the delivery and attainment of objectives – what are the barriers, issues, concerns and challenges. The identification process is an ongoing one which identifies what can possibly affect the achievement of objectives.

3.1.2 As RM also involves exploring the potential opportunities arising from uncertainty, risk identification can consider events which may accelerate or create attainment of objectives.

3.1.3 Risk identification should take place at all levels across the Council, as set out at paragraph 2.1.5.

3.2 IMPORTANCE OF OBJECTIVES

3.2.1 A key principle of effective RM is that all risks are related to, and based upon, objectives. The Council's strategic priorities and objectives are set out in the Council Strategic Plan 2017 – 2022[6], Services' Annual Service Improvement and Performance Reports (ASPIRs)[7] and other strategies and plans.

3.2.2 It is imperative that objectives are clear and understood as they are the basis for the RM process.

3.3 RISK IDENTIFICATION TECHNIQUES

3.3.1 The following are examples of techniques that may be used to identify risks:

- Drawing on previous experience;
- Review of key Council documentation including strategies and plans e.g. Council Strategic Plan, Service ASPIRs etc.;
- Inspection reports and feedback from regulators / standard setters / auditors etc.;
- Results of self-assessment exercises, e.g. EFQM etc.;
- SWOT analysis – considering the strengths, weaknesses, opportunities and threats in terms of the Council, Service, Service-area, project and specific objective in question;
- PESTLE analysis – considering political, environmental, social, technological, legal and economic drivers of the objective and the risks each may present;
- Performance indicators;
- Group sessions, workshops and horizon scanning to engage and consult with relevant parties;
- Questionnaires issued seeking a wide range of views on top risks facing the Council;
- Interviews with all levels of management and staff – it is important to have a variety and balance of input from senior managers as well as staff engaged in service delivery and who

6 https://www.glasgow.gov.uk/CHttpHandler.ashx?id=40052&p=0

7 http://connect.glasgow.gov.uk/article/15797/ASPIR (intranet link not available to non-Council users)

may have more practical experience and understanding of issues 'on the ground';
- External engagement and benchmarking with other local authorities and organisations, and
- Bow tie analysis – explained in further detail in section 3.6.

3.4 RISK CATEGORIES

3.4.1 Once identified, risks can also be categorised by type, as follows:

• Political	• Reputational
• Economic / financial	• Physical / assets
• Social	• Contractual
• Technological	• Environmental
• Legislative / regulatory	• Operational
• Vision and values	• Transformation / change
• HR / people	• Integrity

3.4.2 It is common for risks to cross a number of categories however, best practice is for each risk to be categorised according to the type to which it is **most closely** aligned.

3.5 DESCRIBING RISKS

3.5.1 All risks should be crafted to detail the risk, cause and effect:

Risk: A brief description of the event or the potential threat (or opportunity).
Cause: The drivers or triggers that may lead to the realisation of the risks / uncertainty.
Effect: The consequences that may arise from the risk / uncertainty materialising.

3.5.2 Risk descriptions themselves are often prefaced with:

"Loss of…." *"Lack of…."* *"Failure to…."*

"Inability to…." *"Reduction of…."* *"Disruption to…."*

"Inappropriate…."

Describing Risk - Example:

Risk: Failure to deliver major change projects on time and on budget.
Cause: Lack of, or ineffective, project management; under-estimation of resource requirements; lack of appropriate resources; conflicting priorities.
Effect: Financial pressure; detrimental impact to deliverability of other parts of the programme; increase in temporary staffing costs.

3.6 BOW TIE ANALYSIS

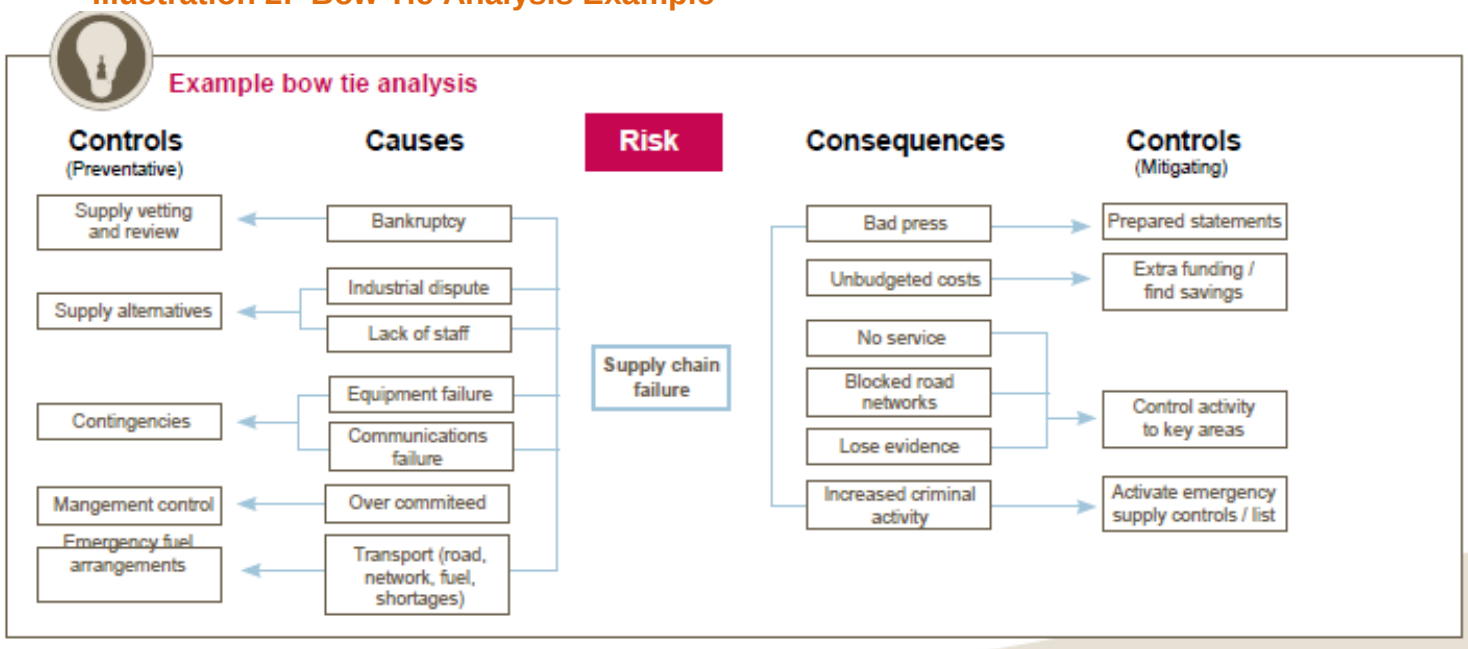
3.6.1 Bow tie analysis is a visual technique used to identify the potential causes and triggers of risks and the resultant consequences that may arise. The analysis also requires identification of the safeguards and preventative barriers that can be put in place to stop or reduce the chance of the risk arising and the reactive, mitigating actions that can be put in place to control the impact of the risk in the event that is does occur.

3.6.2 The approach is a logical one that firstly requires an understanding of the objective and the risk to it. This is the central 'knot' of the bow tie. To the left hand side are threats and events that could lead to the risk event. It is these threats that should be prevented by safeguards and control actions. To the right hand side of the diagram are consequences. These are the worst case results if the event occurs and there are no mitigating actions in place to stop it or mitigate against it.

3.6.3 Both types of barrier, preventative and mitigating, should be specific and their performance / implementation verifiable. Specific details are of the essence when using bow tie analysis – they should be ideally be prepared in a workshop environment with a range of participants.

3.6.4 Training has been provided to members of the Council's RM community on this model and materials and guidance can be obtained from Corporate Governance. Illustration 2 below is an example of a bow tie analysis in the context of the risk of supply chain failure.

Illustration 2: Bow Tie Analysis Example[8]



3.7 RECORDING RISKS – RISK REGISTERS

3.7.1 Risk Registers are means of recording identified risks and associated information and are the primary tool for effective RM in the Council. The Council has developed a standard Risk Register template which can be found in **Appendix 1**. This is also supported by a quick reference guide on how each part of the template should be completed.

[8] ALARM Risk Management Toolkit (2016) https://www.alarm-uk.org/

3.7.2 All Council Risk Registers must adopt this format. Where additional information may be useful, this can be added but the base contents are as follows:

- Risk reference
- Risk status (open or closed)
- Date identified
- Risk title
- Risk description (risk / cause / effect)
- Risk owner (see sections 5.4 and 8.10)
- Responsible officer (see section 5.4)
- Risk category (see section 3.4)
- Risk treatment approach (4T's) (see section 5.3)
- Alignment to the Council's Strategic Plan
- Specific objective linked to each risk
- Inherent assessment (impact x probability)
- Control and mitigating actions
- Residual assessment (impact x probability)
- Planned next steps and future actions
- Change in residual risk scoring in the review period
- Date last reviewed
- Date of next review

3.7.3 In accordance with the various levels of risk management across the Council, the following separate Risk Registers will be developed and maintained:

- Corporate Risk Register (CRR) for strategic risks i.e. uncertain events that may negatively impact the achievement of the Council's vision and strategic objectives;
- Service Risk Registers (SRRs) for operational risks – uncertain events that could negatively impact on the day to day operations of the Service;
- Service-area / team Risk Registers for localised, operational, day to day and staff risks, and
- Programme / project Risk Registers – uncertain events that may impact on the achievement of project or programme objectives.

Further information can be obtained from: corporategovernance@glasgow.gov.uk

Or on Connect at
http://connect.glasgow.gov.uk/article/22018/Risk-Management

SECTION 4 RM STAGE 2: ANALYSE AND ASSESS RISKS

4.1 RISK ANALYSIS AND ASSESSMENT

4.1.1 Once risks have been identified, they must be assessed in terms of how likely it is that they will materialise (**probability**) and, if they do, what might the effects be (**impact**). Every risk will be considered as unique, with its own magnitude and significance. The Council has only finite resources to manage risk, therefore the process of assessing risks provides a means of prioritisation and optimising responses to risks. Decisions on appropriate action and the allocation of resources will then be based on this assessment.

4.1.2 Risk is assessed as a product of probability and impact. A Risk Assessment Matrix has been developed (set out in Illustration 3) which specifies the values to be attributed to each risk for both of these elements. This is a '5x5' matrix and the assessed scores of impact and probability are multiplied together to determine the overall risk score, to a maximum of 25.

Illustration 3: Corporate Risk Assessment Matrix

PROBABILITY							
	Almost certain	5	5	10	15	20	25
	Likely	4	4	8	12	16	20
	Possible	3	3	6	9	12	15
	Unlikely	2	2	4	6	8	10
	Rare	1	1	2	3	4	5
			1	2	3	4	5
			Negligible	Minor	Moderate	Major	Critical

4.1.3 Within Risk Registers, each risk will be assessed twice: once in terms of inherent risk and then in terms of residual risk.

4.1.4 To assess **inherent risk**, the impact and probability must be considered in the absence of any controls: what is the level of risk before controls are considered, what is the susceptibility of the Council to risk, in the first instance? Inherent risk assessment is intended to demonstrate the purpose and effect of control and mitigating actions – it will show the exposure in the event that control and mitigating actions fail.

4.1.5 An assessment of **residual risk** then follows and takes into account the control and mitigating actions identified. Where there is no change in the assessed risk score between inherent and residual, this is generally indicative of a lack of, or ineffective controls or circumstances where the Council is limited in the action it can take.

4.1.6 Risk assessment using probability and impact scoring can be subjective therefore, guidance has been developed to assist with the determination of risk scores. This process requires professional judgement and it is best practice to seek a range of views and perspectives when assessing risks.

4.2 ASSESSING PROBABILITY

4.2.1 In assessing probability, the following 1 to 5 scoring system is to be followed:

ASSESSING PROBABILITY			
Score	**Description**	**% of Occurrence**	**Guidance**
5	Almost certain	80 – 100%	Hard to imagine the event not occurring - event occurs regularly
4	Likely	60 – 79%	Probable - more likely to occur than not
3	Possible	35 – 59%	Reasonable chance of occurrence – the event may happen
2	Unlikely	15 – 34%	Not expected to occur and unlikely but still not exceptional
1	Extremely unlikely	0 – 14%	Hard to imagine the event happening, only in exceptional circumstances or once in every 10 years

4.2.2 It is recognised that this assessment is subjective therefore a range of views should be sought as part of the process. It will not be possible to determine an exact chance of occurrence therefore the percentages noted are for guidance only. Reference must be made to experience and information available at the time of assessment.

4.3 ASSESSING IMPACT

4.3.1 In assessing impact the following 1 to 5 scoring system is to be followed:

ASSESSING IMPACT	
Score	**Description of impact on ability to deliver defined objectives**
5	Fundamental / catastrophic
4	Major
3	Moderate
2	Minor
1	Insignificant / negligible

4.3.2 Illustration 4 below provides examples of more detailed impact descriptors. The use of descriptors will assist in ensuring greater consistency when scoring risks however these are indicative only. When using descriptors, each individual objective must be considered on its own merit.

4.3.3 The assessment of impact should be informed with reference to the highest scoring part of the risk i.e. if a risk scores 5 for reputational impact but 4 for all other categories, the risk should be considered to have an overall impact rating of 5.

Illustration 4: Detailed Impact Assessment Descriptors

Categories	1 Insignificant	2 Minor	3 Moderate	4 Major	5 Fundamental
Strategic/ Operational – Impact on objectives and outcomes	Minor and easily recoverable. Minimal disruption.	Some impact but can recover within the short term. Maximum 1 day disruption.	Some impact but more significant outcomes will take a longer time to achieve. 1-3 days disruption.	Significant impact with some non-recoverable aspects of service. 3-5 days disruption.	Unable to fulfil statutory obligations. Extended disruption (5 days plus). Complete failure to deliver outcomes.
Financial Impact	Negligible (< 1% of budget). Containable within section / team.	Minor (1 – 2.5% of budget). Containable within Service.	Some impact but corrective action can be taken (2.5 – 10% of budget).	Financial performance seriously affected (10 – 25% of budget).	Financial performance critically compromised (> 25% of budget).
Reputational	No interest to the press or damage to public reputation. Complaints.	Some adverse publicity and minor damage to reputation. Local media.	Longer term impact of negative publicity. Moderate reputational impact. Regional media.	National media	Negative media longer than 5 days. International media.
Staff	Minimal disruption to staff - retention remains as expected	Minor staff impact and minimal disruption to staff	Staff unrest and small pockets of industrial relations breakdown	Industrial action. Unable to recruit skilled staff for key roles for an extended period.	Prolonged industrial action ceasing material parts of services. Sustained loss of key staff groups.
Regulatory/ Health and Safety	Minor internal breach. Trivial injury(ies).	Major internal breach. Minor injury(ies).	Minor external breach. Major injury(ies).	Major external breach. Major Injury(ies).	Stops work. Fatality(ies).
Legal	Small number of individual claims	Moderate number of individual claims.	Ombudsman	Litigation	Multiple litigation.
Environmental	Litter	Non-hazardous	Noxious chemicals	Significant contamination	Major incident
Schedule / Delivery Programme	< 10% overrun	10 – 15% overrun	16 – 25% overrun	26 – 50% overrun	> 50% overrun

SECTION 5 RM STAGE 3: RESPOND TO RISK

5.1 RESPONDING TO ASSESSED RISK SCORES

5.1.1 Once risks have been scored using the Risk Assessment Matrix, the next step is to understand what this score means and use it to inform a suitable response.

5.1.2 Each risk, based on its score, will be rated as either **LOW, MEDIUM, HIGH OR VERY HIGH** and will be colour-coded according to the Risk Assessment Matrix at Illustration 3. This rating will determine the broad approach to be taken to the management of each risk, as set out in Illustration 5. This rating reflects the Council's risk appetite i.e. the level of risk the Council is willing to accept or tolerate which then dictates the level and intensity of response required.

5.1.3 It should be noted that work is ongoing in relation to the determination and application of risk appetite for the Council and this document will be updated in due course as this is agreed.

Illustration 5: Responses to Risk Ratings (1)

Low	- Not a priority for treatment / management - In some situations, it may be acceptable for no mitigating action to be taken - All low risks must still be reviewed to ensure no change to their assessed rating
Medium	- Steps should be taken to address these risks - Medium term plans are required to reduce the risk - Normally, as a general rule, within one year but this should be considered on a case by case basis
High	- To be monitored regularly and closely at a senior level - Action is likely to be required to reduce the probability and/or impact to an acceptable level in the short term
Very High	- Priority risks to be actively monitored by extended senior management - Likely to require action to reduce the probability and/or impact urgently

5.1.4 Illustration 6 shows presents an alternative view of this approach and sets out broad responses to each risk rating, low, medium, high and very high.

Illustration 6: Responses to Risk Ratings (2)

High Probability / Low Impact	**High Probability / High Impact**
- Develop controls if obvious and cost effective - Housekeeping - Monitor on a moderate frequency	- Allocate resource to mitigate and develop strategic response - Avoid - Transfer - Active and frequent monitoring - Escalate and report
Low Probability / Low Impact	**Low Probability / High Impact**
- Accept - Monitor at least every quarter - Develop controls if obvious and cost effective	- Contingency plans - Audit controls - Consider transfer - Monitor regularly

5.2 RISK APPETITE AND TOLERANCE

5.2.1 The Council's strategic risk tolerance is shown on Illustration 3 as the heavy bold line separating the medium and high rated risks.

5.2.2 Risks assessed to the left of that line i.e. low and medium rated risks, are to be monitored and risks assessed to the right of the tolerance line i.e. high and very high rated risks, will require further action as these must be actively managed.

5.2.3 If during review, it is determined that the appetite around certain risks is increased, this can be effected by the relaxing or the removal of control and mitigating actions. However, any such decision must be carefully informed, recorded and reported and shared with other risk owners to ensure a full and common understanding of potential interplays across various risks.

5.3 MANAGEMENT OF RISK

5.3.1 In broad terms, any risk can be managed using any of the '**4 T's**' below:

Risk Treatment	What does it mean?	Examples
Tolerate	Accept the risk and manage within existing resources and arrangements	• If the risk is relatively insignificant • If costs of treatment or transfer are greater than the potential benefits • If ability to respond is limited and out with Council's control • If the risk is acceptable to the Council – generally low rated 'green' risks • Do nothing differently beyond existing controls • Focus on contingency plans

Risk Treatment	What does it mean?	Examples
Treat	Reduce – put in place cost effective control and mitigating actions to reduce the probability of the risk arising; reduce the impact if the risk were to arise, or both	To **reduce probability** (mitigating action): • Staff training to raise awareness of the risk and controls required • Documented procedures and processes with which all staff must comply • Regular monitoring and review of compliance with procedures To **reduce impact** (control action): • Business continuity plans • IT back-up systems • Public relations and media handling
Transfer	Let another party take the risk and cover the costs / losses, should they arise	Through insurance or passing operational responsibility for risk to a partner or contractor
Terminate	Avoid - if the risk is considered too high, do not engage in the activity which presents the risk or undertake the activity in a different way to obtain the same desired result	• Where treatment of the risk would not reduce the risk to an acceptable level • Risk is undesirable • No capacity to manage the risk to an acceptable level

5.3.2 Risk Registers must clearly identify which of these four options is the preferred risk management approach. This will inform the level of control and mitigating actions i.e. those risks identified for treatment will have more extensive and proactive actions than those that are tolerated.

5.4 IDENTIFICATION OF RISK OWNERS AND RESPONSIBLE OFFICERS

Risk Owners

5.4.1 Each identified risk will be allocated a designated Risk Owner. They are accountable for the co-ordination of activity required to manage the risk and for monitoring the risk on an appropriate frequency. Details of the responsibilities of the Risk Owner can be found in section 8.

5.4.2 Risk Owners should be appropriately senior to ensure empowerment and authority to recommend the allocation of resources to manage risks which should then be agreed by either Service senior management or the Extended Corporate Management Team. Risk owners should be listed by name or specific job title on Risk Registers and should be familiar with the risk area and objective in question.

Responsible Officers

5.4.3 As well as a Risk Owner, each risk should have a designated Responsible Officer. This is generally an officer who works alongside the Risk Owner and who is responsible for implementing agreed actions. They will support the Risk Owner.

5.5 TREATING RISKS WITH CONTROL AND MITIGATING ACTIONS

5.5.1 Recall the way in which the Council describes risk using the three elements: risk, cause and effect, as set out in section 3.5. These elements also impact on how a risk can be treated as different approaches can be taken to address both cause and effect as set out in Illustration 7.

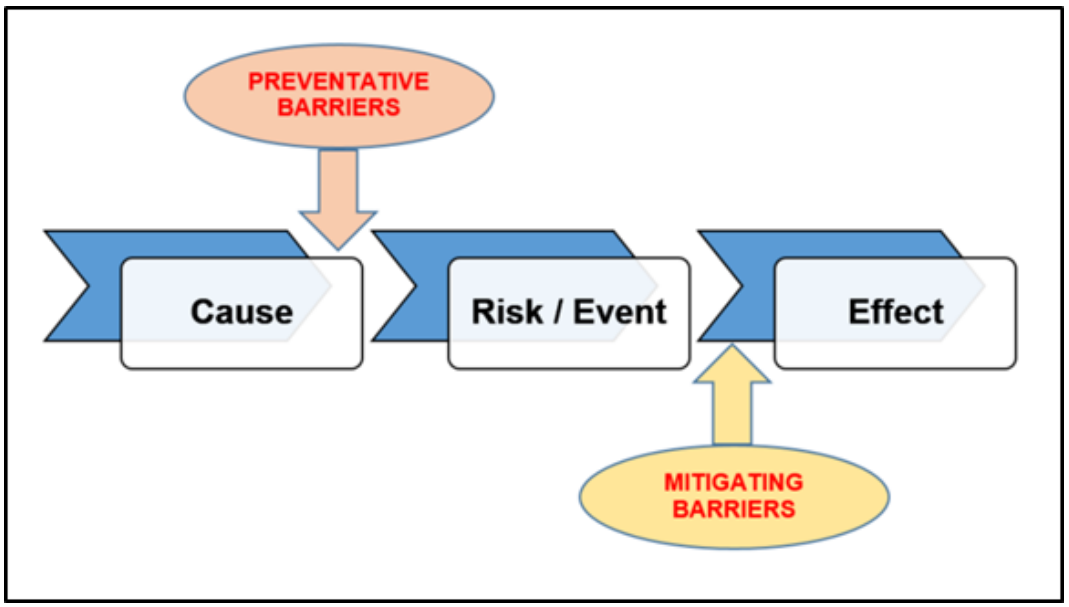
5.5.2 Cause can be considered in terms of **preventative measures** – the potential drivers of risk materialising are understood so cause can be targeted to take steps to stop these from arising i.e. preventative barriers. These measures are aimed at reducing **PROBABILITY**. For example:

- Documented policies and procedures
- Training
- Recruitment
- Risk assessment

5.5.3 Effect can be considered in terms of **mitigating measures** – the event has occurred so focus shifts to how the consequences can be minimised or better managed. These measures are aimed at reducing **IMPACT**. For example:

- Business continuity plans
- Emergency response
- Insurance
- Public relations

Illustration 7: Preventative and Mitigating Barriers



5.5.4 When devising control and mitigating actions, these must be tangible with a clear audit trail as they could be subject to audit.

5.5.5 Control and mitigating actions should be devised with regard to the Council's internal control environment and the range of measures in place to ensure achievement of objectives; completeness and accuracy of processes, and effectiveness of operations.

5.5.6 Additionally, the cost and resource requirements to implement and sustain a mitigation must be considered and balanced against the risk tolerance.

5.5.7 Risk will materialise therefore contingency arrangements must also be identified as part of the response to risk.

5.6 RISK AS OPPORTUNITY

5.6.1 As risk relates to uncertainty, as well as presenting threats, it can also present opportunities. Opportunity risk management involves actively taking advantage of risk through realisation, enhancement and exploitation of opportunities, where there is scope to gain benefit.

5.6.2 In addition to the 4T's of risk treatment, set out at section 5.3, a fifth 'T' applies for 'take' i.e. take advantage of the uncertainty. Opportunities should be considered on a case by case basis and the resources required for their pursuit and realisation determined.

SECTION 6 RM STAGE 4: MONITORING AND REPORTING

6.1 MONITORING RISKS

6.1.1 Risk Registers (as detailed in section 3.7) form the basis of the ongoing and iterative risk monitoring and review process and allow for the identification of trends, progress and action required.

Why Monitor Risk?

6.1.2 The purpose of monitoring and reporting risk is threefold:

- To monitor whether the risk profile of the Council is changing and react accordingly;
- To gain assurance that RM is effective i.e. treatment is addressing risks as expected, and
- To identify further actions required to manage risks.

6.1.3 Risks should not remain static for extended periods of time. The risk profile of the Council is changeable and the effectiveness of the agreed responses to individual risks should also drive changes in assessed risk scores.

6.1.4 Regular monitoring and review of each identified risk is crucial to ensure Risk Registers are up to date. Uncertainty may have in/decreased gradually over time or changed sharply and suddenly in response to extenuating circumstances. Also, as control and mitigating actions are embedded, risk scores may decrease. Monitoring will detect these changes and allow them to be fed into the RM process.

6.1.5 Monitoring and review also allows the Council to learn lessons from events and trends and to ensure the continued appropriateness and effectiveness of identified control and mitigating actions.

6.1.6 Exact requirements and frequencies for monitoring risks will vary depending on the assessed risk score and rating and its position in relation to the Council's risk appetite, as set out in Illustrations 5 and 6.

6.1.7 A key part of the review and monitoring process is the consideration of effectiveness. Once control and mitigating actions are identified and implemented, if this has proven ineffective in reducing the risk scoring, alternative or additional measures will be required.

6.1.8 The review of Risk Registers should be documented to provide an audit trail of discussions and agreed changes in the reporting period. This need not be onerous and could be as simple as the addition of a column, for internal use only, within the Risk Register, setting out the agreed changes to individual risks and recording where risks have been escalated.

6.1.9 Alternatively, separate control sheets / reports can be prepared, approved and retained for each review. These should detail the discussions undertaken as part of the review; new risks identified; closed risks; changes to risk descriptions and assessed risk scores and any updates to control and mitigating actions. Also, any decisions on escalations should be documented.

6.2 ESCALATING AND REPORTING RISK

6.2.1 The multi-level risk structure operated by the Council, as set out in section 2.1.5, provides for a top down approach driven by corporate and Service objectives but one which also ensures clear routes for escalation of risks between levels and ensures the alignment of strategic and operational risks.

6.2.2 Individual risks cannot be considered in isolation as they may have a bearing on others – this is why clear escalation and reporting routes are important – to ensure awareness and maximise efficiency of control and mitigating actions which may be able to tackle more than one risk simultaneously.

6.2.3 **Project / Programme Risk Register**:

- Used to record, monitor and manage risks associated with specific initiatives, projects or major programmes.
- Owned by the project / programme manager.
- Should be reported to the project / programme Board on a regular basis, at least quarterly however, more frequent reporting should be implemented depending on the project / programme timescales and progression rates i.e. where a programme / project is relatively short term in nature, increased reporting frequency will be required.
- Where a project is part of a wider programme, very high project risks should be escalated to the Programme Management Office, or equivalent, to determine any wider impacts.

Further information on the Council's approach to managing projects can be found in the Corporate Project Management Toolkit, available on Connect at http://connect.glasgow.gov.uk/toolkit

Or from corporategovernance@glasgow.gov.uk

6.2.4 **Service area / function / team Risk Register:**

- Should be a standing item on the agenda of team / Service-area meetings, with a formal review on a quarterly basis, at least or following significant service or structural changes.
- Owned by the relevant Head of Service, supported by Service-area managers.
- Very high risks and those identified for escalation should be fed into the Service Leadership or Senior Management Team for discussion and consideration of wider Service impact.

6.2.5 **Service Risk Register:**

- Should be a standing item on the agenda of the Service Leadership or Senior Management Team with a formal review on a quarterly basis, at least or following significant service or structural changes.
- Owned by Service Directors who should seek assurance from Risk Owners that their assessment remains current and that risk is being effectively monitored and managed.
- On a quarterly basis, updated Service Risk Registers should be submitted to Corporate Governance.
- May include escalated risks from Service-area/function/team Risk Registers.
- Very high risks should be discussed at the Operational Risk Management Forum and considered for escalation into the Corporate Risk Register.

6.2.6 **Corporate Risk Register**:

- Sets out the strategic risks to the Council.
- Maintained by Corporate Governance in conjunction with Risk Owners and the Operational Risk Management Forum (ORMF) and reviewed on a quarterly basis.
- May include risks escalated from Service-level Risk Registers.
- On a bi-annual basis, reports are presented to the Extended Corporate Management Team and the Finance and Audit Scrutiny Committee (FASC). The position as at 31 March is generally reported in May and the position as at 30 September generally reported in November.

6.2.7 It is important that where significant emerging or escalating risks are identified out with the scheduled reporting periods, these should be discussed with Service Directors and Corporate Governance as soon as possible.

6.3 REVIEW – POINTS FOR CONSIDERATION

6.4 SUMMARY OF RISK REPORTING

6.4.1 The table below sets out a summary of the formal reporting requirements in relation to Risk Registers. These are set out as a minimum.

Risk Register / Report	Responsible	Reported To	Frequency
Corporate Risk Register	Compliance Manager	ECMT and FASC	Bi-annually
Service Risk Register	Service Risk Management Champion	Service Leadership / Senior Management Team and Corporate Governance	Quarterly (at least)
Service area / function / team Risk Registers	Team Manager	Head of Service and Service Risk Champion (for consideration in the Service Risk Register)	Quarterly (at least)
Project / Programme Risk Registers	Project / Programme Managers	Project / Programme Boards (and other agreed parts of applicable governance structures – see Project Management Toolkit)	Quarterly (at least)

SECTION 7 RM STAGE 5: INTEGRATING RISK MANAGEMENT

7.1 INTEGRATION OF RISK MANAGEMENT

7.1.1 RM must not be seen simply as an operational issue – it must be considered when the Council is developing policies and strategies and be an integral part of project and programme planning. In short, RM should be integrated with the Council's strategic planning and performance management arrangements. As strategic plans and objectives are developed, risks should be identified and recorded at a Service and corporate level.

7.1.2 It is important that Service Directors and managers integrate the functions of planning and RM. They should also retain flexibility within budgets and resource allocations to allow control and mitigating actions to be implemented, as required. RM may also highlight scope for efficiencies, perhaps where risks are over-managed and control and mitigating actions are beyond the level required and can therefore be scaled back presenting a possible financial saving and/or the ability to reallocate staff.

7.1.3 A key element of the RM process is learning lessons about the organisation: to be effective and fully embedded, RM should feed into the business planning process and the knowledge gathered from RM used to inform the future.

SECTION 8 ROLES AND RESPONSIBILITIES

8.1 ELECTED MEMBERS AND COUNCIL COMMITTEES

- Understand risk management arrangements and consider the implications of risk during decision making and policy approval
- Through the relevant Committee(s):
    - oversee the effective management of risk
    - monitor the adequacy of the Council's overall risk management arrangements
    - receive regular reports from the Director of Governance and Solicitor to the Council on risk management arrangements

8.2 CHIEF EXECUTIVE

- Endorse and promote the RM Policy and Framework
- Ensure a Corporate Risk Register is established and maintained

8.3 EXTENDED / CORPORATE MANAGEMENT TEAM

- Approve the RM Policy and Framework, including the Council's risk appetite i.e. the level of risk it is prepared to tolerate
- Champion and support the implementation of the RM Policy and Framework and creation of a culture where RM is embedded, valued and effectively undertaken
- On a six-monthly basis, formally review the key risks facing the Council included in the Corporate Risk Register, specifically considering their importance against strategic objectives, and the associated controls
- Ensure that consideration is given to identifying and managing risks associated with the delivery of the Council Plan and major strategic initiatives
- Support the activities of the Operational Risk Management Forum
- Ensure that all strategic risks are effectively managed and undertake the role of Risk Owner, as appropriate

8.4 DIRECTOR OF GOVERNANCE AND SOLICITOR TO THE COUNCIL

- Promoting and champion the application of the RM Policy and Framework
- Ensuring appropriate resources are allocated to support the Elected Members, Services and Council officers in the effective implementation of the Policy and Framework
- Receive from Corporate Governance reports on compliance with the RM Policy and Framework and act as an escalation point for any issues of non-compliance

8.5 SERVICE DIRECTORS

- Ensure that RM is embedded at all levels within their area of responsibility
- Manage strategic and operational risks within their Service to safeguard employees and service users, protect assets and preserve and enhance service delivery to the population
- Ownership of specific risks within the Corporate Risk Register, as appropriate
- Maintain the effective stewardship of public funds and the promotion of a favourable corporate image
- Establish and maintain a Service Risk Register
- Allocate sufficient resources to allow for effective RM within the Service

8.6 SERVICE LEADERSHIP / SENIOR MANAGEMENT TEAMS

- Ensure risk is managed effectively at all levels in each Service area
- Monitor the Service Risk Register with formal reports reviewed on a regular (at least quarterly) basis
- Ensure risk management is linked to Service Annual Service Plan and Improvement Reports (ASPIRs) and major programmes and projects etc.
- Ensure compliance with the Corporate Risk Management Policy and Framework
- Support the RMCs (as per section 8.13)

8.7 HEAD OF AUDIT AND INSPECTION

- Review the effectiveness of the RM Policy and Framework and Services' compliance with it
- Review the progress with the implementation of mitigating and control actions
- For the purposes of the Annual Internal Audit Report, consider whether RM is being effectively delivered throughout the Council

8.8 CORPORATE GOVERNANCE

- Responsible for the development, maintenance and ongoing review of the RM Policy and Framework
- Support Elected Members, Services and Council officers in the effective implementation of the RM Policy and Framework
- Co-ordinate the Council's RM activity
- Develop, maintain and report on the Council's Corporate Risk Register
- Prepare and present six-monthly reports to the Extended Corporate Management Team and, on behalf of the Director of Governance and Solicitor to the Council, to relevant Council Committee
- Assist in providing support and training on RM
- Chair the Operational Risk Management Forum
- Hold Services to account for implementation of the RM Policy and Framework, including challenging agreed actions and risk assessments
- Promote and facilitate the sharing of risk information and best practice across the Council Family
- Seek assurance from Services in respect of their adherence to and compliance with the Framework. This will be discussed at the Operational Risk Management Forum and reported to the Director of Governance and Solicitor to the Council.

8.9 SERVICE MANAGERS

- Effectively identify and manage risk within their particular Service areas
- Implement the Council's RM Policy and Framework across their area of responsibility
- Work with Service Risk Management Champions to ensure relevant information is captured on Risk Registers, updated, escalated and reported as required

8.10 RISK OWNERS

- Managing all aspects of assigned risks
- Obtaining additional resource or support as required to manage and monitor assigned risks
- Ensuring assigned risks are regularly updated in Risk Registers
- Determining the actions required to mitigate risks and ensuring these are implemented fully and effectively and ensuring the impacts of these measures on risk scoring are reflected

8.11 FINANCIAL SERVICES INSURANCE SECTION

- Identifying financial exposure to the Council's Insurance Fund through claims monitoring
- Reporting of claims data to Heads of Service
- Identifying risk exposures through claims monitoring

8.12 EMPLOYEES

- Monitor their own functions/teams on an ongoing basis to identify new and emerging risks and escalate as necessary, in line with this Framework
- Report events, incidents or accidents which could expose the Council to risk
- Make every effort to be aware of situations that may place themselves or others at risk and report identified hazards
- The following areas are typical of those in which care must be exercised at all times:
    - slips, trips or falls
    - working at height
    - manual handling etc.
    - driving while on Council business
- Ensuring, alongside line management, that appropriate training has been completed to carry out their duties

8.13 RISK MANAGEMENT CHAMPIONS

8.13.1 Each Council Service will designate an appropriate officer as its Risk Management Champion (RMC). Services will also identify appropriate deputes. RMCs must be supported by Senior Management within their Service to ensure the importance of RM is understood and embedded across the Service.

8.13.2 RMCs are responsible for supporting the compliant implementation of the RM Policy and Framework by ensuring that:

- the RM process is championed and adhered to consistently across the Service
- Risk Registers are developed, maintained and regularly reviewed (at least quarterly) for sections/teams/functions
- an overall Service Risk Register (SRR) is developed, maintained and regularly reviewed (at least quarterly)
- SRRs are reported to the Service Leadership / Senior Management Team on a quarterly basis
- SRRs are provided to Corporate Governance on a quarterly basis
- arrangements are in place for RM information and guidance to be communicated to all relevant staff

8.14 OPERATIONAL RISK MANAGEMENT FORUM

- Promote a risk management culture at all levels within the Council, ensuring it is a key consideration in decision making and governance
- Provide a forum where Service-level risks can be discussed and considered for escalation into the Corporate Risk Register
- Identify and assess risks and mitigating actions for inclusion in the Corporate Risk Register
- Review, as a minimum every 6-months, the Corporate Risk Register
- Champion the corporate approach to risk management and business continuity
- Develop, share and promote information and best practice about risk management and business continuity across the Council Family
- Provide a forum for updating and reviewing the Council's risk management and business continuity policy and strategy arrangements, including associated corporate templates
- Co-ordinate the development and implementation of a training, testing and exercising programme for business continuity
- Engage with and support Corporate Governance in leading the Council in risk management and business continuity
- Engage with Corporate Governance with respect to technological solutions for risk management and business continuity

SECTION 9 GOVERNANCE AND COMPLIANCE

9.1 INTERNAL AUDIT

9.1.1 Compliance with this RM Framework may be subject to review by the Council's Internal Audit section. Such reviews will generally be intended to provide assurance to Elected Members and senior management that the control environment around the operation of the Framework is effective. The findings from these reviews will be presented to the relevant Council Committee.

9.2 LINKS TO BUSINESS CONTINUITY

9.2.1 The relationship between RM and Business Continuity Management is a circular one: in completing RM processes, Services will identify information that should be reflected in their business continuity management arrangements and vice versa e.g. contingency plans identified as a response to risks if they occur.

9.2.2 The Council's Business Continuity Management Policy and Framework[9] provides detailed guidance on the steps Services are required to take to ensure the Council can continue to operate and provide services, even in times of crisis or during a serious disruptive incident.

9.2.3 In developing and maintaining Risk Registers, Services must refer to their Business Continuity management materials, including Business Impact Analyses and Business Continuity Plans, to ensure these reflect functions and activities which are essential to service delivery and operations and what is required to mitigate the risks associated with them being disrupted.

9.3 BEST VALUE

9.3.1 RM and Best Value (BV) share a number of common goals. They are both based on principles of quality management; they require a co-ordinated and integrated approach across all areas of corporate activity, and everyone in the chain of service needs to be involved in the process.

9.3.2 Best Value cannot be delivered unless the organisation's assets and objectives are protected. RM is a system for controlling all risks that threaten the assets and objectives of the authority and so the two concepts form a valuable partnership. To achieve this there is a requirement at all levels for clear and effective communication and that the escalation procedures are strictly adhered to.

9.3.3 Along with achieving BV, this Framework will help ensure that the Council maintains the effective stewardship of public funds; maintains sound corporate governance, and protects the Council's corporate image.

9.3.4 To ensure continuous improvement in RM, the Policy and Framework will be kept under review.

[9] http://connect.glasgow.gov.uk/article/13127/Business-Continuity

SECTION 10 DOCUMENTATION AND RECORDS MANAGEMENT

10.1 The following documentation will be generated through the implementation of the RM Framework:

- Corporate Risk Register;
- Service Risk Registers;
- Service/function/team level Risk Registers;
- Programme and project Risk Registers;
- Section/function/team level Business Impact Assessments (BIAs);
- Service-level Business Impact Assessments (BIAs);
- Section/function/team level Business Continuity Plans (BCPs);
- Service-level Business Continuity Plans (BCPs);
- Reports to relevant Council Committees, Extended Council Management Team and Service Leadership / Senior Management Teams;
- Internal Audit Terms of Reference, and
- Internal Audit reports.

10.2 All RM related documentation will adhere to the Council's Records Management arrangements and Information Security guidelines.

10.3 A dedicated area has been set up on EDRMS to store all risk management materials and information. This will provide appropriate access and distribution control. This area will be overseen by Corporate Governance and each Service will be provided with its own secure folder in which to save relevant RM documentation, including Service Risk Registers.

10.4 Services should not store RM documentation locally: all RM material must be held in the dedicated area.

Any queries on this document can be directed to:

Corporate Governance Compliance
City Chambers
Glasgow
G2 1DU

Tel: 0141 287 3771
e-mail: corporategovernance@glasgow.gov.uk