ARMAGH CITY, BANBRIDGE & CRAIGAVON BOROUGH COUNCIL	
Document Reference Number:	GPR/P9.0/V2.0
Title of Policy:	Risk Management Policy
No of Pages (including appendices):	10
Version:	Two
Issue Date:	February 2017
Policy Nominated Officer:	Martina McNulty
Equality screened by:	Mary Hanna
Equality screening date:	Original version screened on 30 October 2014
Amendment Version Issue Date:	**March 2021**
Sent out by:	**Martina McNulty**
Approved by:	**Roger Wilson**
Review Date:	**January 2023**

AMENDMENT RECORD SHEET

Remove and destroy old pages. Insert new pages as indicated.

Revision Number	Page Number	Date Revised	Description of Revision
		February 2021	Review of entire document against the revised Orange Book.
		February 2017	Review of entire document and removal of sections on the assurance framework and stewardship certificates

CONTENTS

1.   INTRODUCTION

Risk Management is about managing threats and opportunities so that the Council is in a stronger position to deliver its objectives and is an essential business tool that encourages innovation and enterprise, not risk adversity. Risk Management includes identifying and assessing risks and then responding to them to ensure effective controls are in place. Failure to manage risk effectively may result in financial losses, disruption to services, bad publicity or claims for compensation.

All organisations face risk or obstacles to achieving their objectives. In order for Armagh City, Banbridge and Craigavon Borough Council (ACBCBC) to deliver its objectives it is important to:

- Understand the nature of the risks we face;
- Be aware of the extent of these risks;
- Identify the level of risk that we are willing to accept;
- Assess our ability to control or reduce the risk; and
- Implement corrective actions.

Risk management should be explicitly linked to the business planning process to ensure it is embedded across the Council. For the risk management process to be effective, the following principles should be applied:

- Risk management should be an essential part of **governance and leadership**, and fundamental to how the organisation is directed, managed and controlled at all levels;
- Risk Management should be an **integral** part of all organisational activities to support decision-making in achieving objectives.
- Risk management should be **collaborative and informed** by the best available information and expertise.
- Risk Management processes should be **structured** to include risk identification and assessment, risk treatment, risk monitoring and risk reporting.
- Risk Management should be **continually improved** through learning and experience.

2.   PURPOSE

This document defines Armagh City, Banbridge and Craigavon Borough Council's Risk Management Policy and describes the process for identifying and managing risk within the Council. It draws on the principles and approach set out in 'The Orange Book, Management of Risk – Principles and Concepts', revised by HM Treasury in 2020 and the NIAO 'Good Practice in Risk Management' (June 2011).

The Local Government Regulations (NI) 2006 (Accounts and Audit) requires the Council to have in place adequate and effective arrangements for the management of risk and to report on these arrangements within the annual governance statement, which forms part of the statutory accounts and which must be considered and approved by Council.

Risks will be managed at one of three levels:

- **Corporate/Strategic Risks –** High level risks which could have a major impact on the Council's corporate plan objectives. These risks will be managed primarily by the Executive Management Team (EMT) and Heads of Department (HOD) and will be subject to challenge by the Performance and Audit Committee.

- **Departmental –** Risks which could impact on the delivery or timescale of activities or deliverables at Departmental level. These risks will be managed by the HOD and may be escalated to corporate level as appropriate.

- **Project Risks** will also exist and these will be managed by the appropriate Project Officer(s). The mechanisms in place for monitoring and reporting risk will vary according to the size and complexity of the project, ranging from the use of a risk register to the appointment of a risk manager.

3.   RISK MANAGEMENT PROCESS

The diagram below shows the key elements of the risk management process.
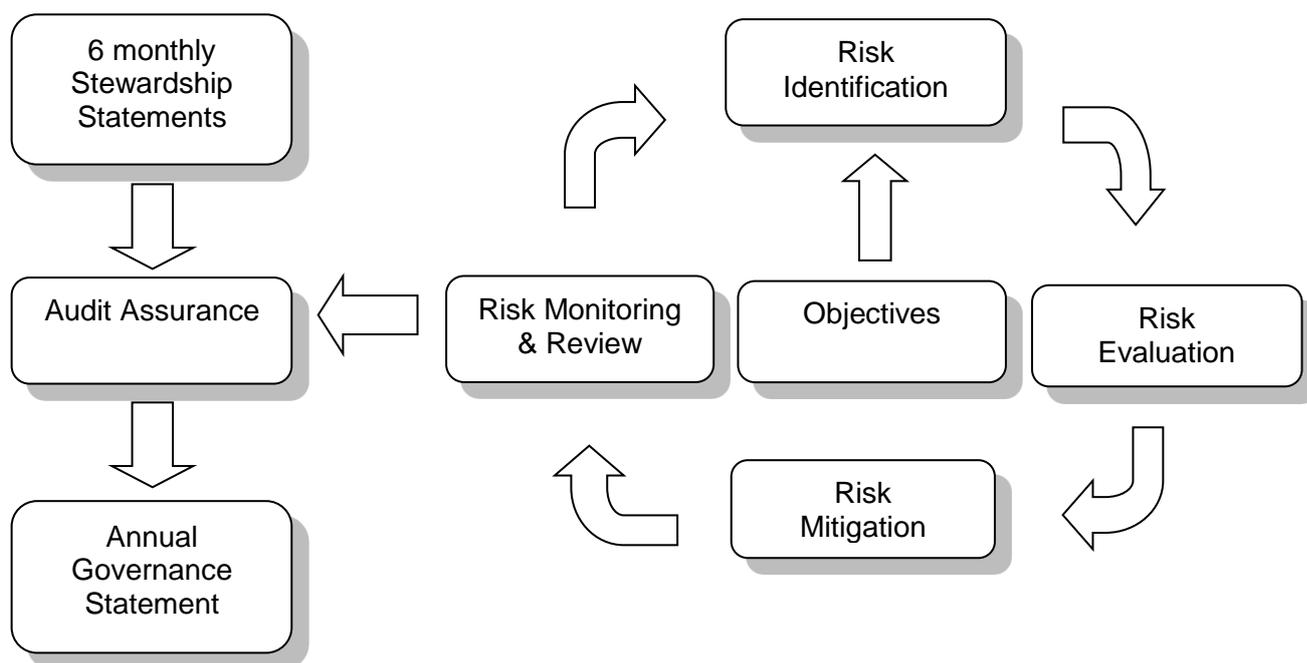
RISK IDENTIFICATION

Risks should be related to objectives as set out in the Corporate, Departmental and Project Plans as appropriate. Some risks may be relevant to more than one objective. However, risk identification and assessment should not be confined to the process of drawing up Plans.

In identifying risks, managers should not just consider threats to the achievement of their objectives but also consider, missed opportunities for improved performance and enhanced capacity. Examples of common risk categories are included at **Appendix 1**.

The standard format Risk Register is illustrated at **Appendix 2**.

EVALUATION OF RISKS

A risk matrix is used to evaluate the risks so that there is an understanding of the risk exposure faced, which in turn influences the level of risk treatment that should be applied to manage/reduce/prevent the risk from occurring. The matrix used for evaluating risk is shown in the diagram below. Risk analysis is primarily concerned with quantifying risk in terms of frequency and severity.

The Council will adopt a consistent approach to evaluating the likelihood and impact of key risks in terms of both:

Likelihood   -   The chance of the risk materialising

 Impact   -   The effect of the risk should it materialise

The likelihood and impact of each risk should be evaluated on a scale of 1 to 5 as set out at **Appendix 3 & 4** to arrive at the overall risk rating.

Two evaluations will be carried out for each risk:

Inherent Score   Risk rating assumes no controls are in place
Residual Score   Risk rating takes into account the controls

Impact	5 (Catastrophic)	5	10	15	20	25
	4 (Major)	4	8	12	16	20
	3 (Moderate)	3	6	9	12	15
	2 (Minor)	2	4	6	8	10
	1 (Insignificant)	1	2	3	4	5
Likelihood		1 (Rare)	2 (Unlikely)	3 (Moderate)	4 (Likely)	5 (Almost Certain)

LOW	MEDIUM	HIGH	UNACCEPTABLE

RISK APPETITE

The risk evaluation should then be compared to the risk appetite for each risk type. While the Council deems any unacceptable risks intolerable it is envisaged that all other risks will be managed in accordance with the risk appetite.

The risk appetite sets out the level of risk that management is prepared to accept, tolerate or be exposed to at any point in time. The risk appetite may vary depending on the category of risk. In some areas the Council may take more risk in order to support innovative thinking, in other areas the Council may take less risk to ensure legal compliance or to maintain public confidence.

Our approach to risk taking will be dependent upon the nature of the risk. Particular care is needed in taking action that could:
- Impact on the reputation of the Council
- Impact on performance
- Results in censure/fines by regulatory bodies
- Results in financial loss/fraud

The target level of risk score will depend on whether the Council is risk averse, risk neutral or risk open.

Risk Appetite	Definition
Risk Averse	Avoid/Mitigate its exposure to risk
Risk Neutral	Moderate appetite to accept exposure to risk
Risk Open	Accepts the impact of the potential risk in materialising

While the Council deems any unacceptable risks intolerable it is envisaged that high scoring risks will be actively managed.

Any risk that has a residual risk score assessed to be low will be considered to be acceptable and will require no further action other than to ensure that the existing controls are operating effectively.

RISK MITIGATION

Once a risk has been identified and evaluated consideration must be given to the appropriate action. The level and type of treatment for each risk will depend on the level of residual risk and the tolerance to the specific risk. The following options are available:

Treat the Risk
Treating the risk means identifying additional actions to be taken that will reduce the likelihood and/or the impact if the event occurred. It is anticipated that the greatest number of risks will fall into this category.

Transfer the Risk
Transfer the risk means using an insurer or third party to cover the cost or losses and share the risk should a risk materialise.

Tolerate the Risk
It may be appropriate to tolerate the risk without any further action for example due to either a limited ability to mitigate the risk or the cost of mitigation may be disproportionate to the benefit gained.

Terminate the Risk
Terminating the risk means ceasing the activity because modifying it or controlling it would not reduce the risk to an acceptable level.

The selected risk response will be captured in the additional action section of the risk register template. The Risk Owner should ensure that responsibility for each action in is assigned to a named individual along with realistic target dates. It is important that any action taken is proportional to the risk. Additional actions highlighted in the risk register templates should link with the actions set out in the individual business plans.

RISK MONITORING AND REVIEW

The Council's Risk Registers are an integral part of the Assurance Process and reporting thereof is the means by which the Council and Performance and Audit Committee can assess the effectiveness of the controls and assurances given for the management of the risks identified.

Risk management should be a continuous process which identifies new risks, changes in existing risks and risks which are no longer relevant.

The risk registers should be reviewed on a *Quarterly* basis via the Council's Risk Management software and updated accordingly, taking cognisance of the outcome of

completed risk actions and any resultant change in risk score or risk classification. Risk actions that have been completed should be transferred to controls.

Evidence to assess effectiveness of controls should be detailed in the risk register template. This enables an opinion on the adequacy and effectiveness of the control and provides assurance on the management of these risks by focussing on the three lines of defence.

These three lines of defence include:

- *Operational Management* - This comes direct from those responsible for delivering specific objectives or operations (i.e. direct management); it provides assurance that performance is monitored, risks identified are addressed and objectives are being achieved.

- *Management oversight* – separate from those involved in the operational delivery but who is actively involved in overseeing and managing risks.

- The third line of defence relates to *independent* and more objective assurance, for example the provision of assurance by Internal Audit.

4.   ROLES AND RESPONSIBILITIES

While the identification of risks is the responsibility of all Council employees and Members, the following groups are noted for their particular role and associated responsibilities in the risk management process:

PERFORMANCE AND AUDIT COMMITTEE

The role of the Performance and Audit Committee is to ensure that there is a risk management process in place and report to the Council members. The Committee will review the Councils approach to risk management and give independent assurance on the adequacy of the Council's risk management policy and the associated control environment.

The Corporate Risk Register will be presented at each Performance and Audit Committee. In addition to this the Departmental Risk Registers of a Directorate will be presented on a rotational basis along with any relevant project risk registers.

RISK OWNERS

The following people are assigned Risk Owners:

- Corporate   Risk Owners allocated by   CE/Strategic Director
- Departmental   Risk Owners allocated by the   HOD
- Project   Risk Owners allocated by the   Project Director/Manager

Risk Owners will have authority to assign resources to manage key risks within defined approvals. They are responsible for managing assigned risks by ensuring controls are in place and properly actioned at all levels. They are also responsible for communicating progress, identifying control weaknesses and recommending remedial actions and ensuring that a suitable system of internal control operates in their area of responsibility.

The EMT and HOD will be responsible for ensuring that the risk management processes become embedded in the culture of the Council through provision of roll out training and facilitation by the Performance and Audit Department.

PERFORMANCE AND AUDIT DEPARTMENT

The Performance and Audit Department can provide guidance on how to identify risks through one to one meetings or facilitated workshops/group discussions.

For new risk registers, the Business Continuity/Risk & Customer Relations Officer can facilitate, if required, the drafting of the risk register with the relevant HOD using the standard template and forward to the relevant person/group for review and agreement. The relevant person/group is then responsible for keeping the risk register up to date and developing the related risk action plans, using the standard template.

For existing registers, on a quarterly basis as required the Business Continuity/Risk & Customer Relations Officer will meet with Risk Owners and provide advice and guidance on the risk registers and action plans and prepare quarterly update reports to the Performance and Audit Committee.

The Internal Audit Manager will undertake the following in respect of risk management:

- Provide an annual independent, objective assessment/opinion of the effectiveness of the risk management and control processes operating within the Council which feeds into the Council's Annual Governance Statement;

- Ensure that the Internal Audit activity is focused on the key risks facing the Council; and

- Provide advice and guidance on risk and control to EMT and HOD and ensure key actions to manage the identified risks are reflected in the relevant risk registers.

COMMON RISK CATEGORIES   **Appendix 1**
(as per HM Treasury Orange Book)

Strategy	Risks arising from identifying and pursuing a strategy, which is poorly defined, is based on flawed or inaccurate data or fails to support the delivery of commitments, plans or objectives due to a changing macro-environment.
Governance	Risks arising from unclear plans, priorities, authorities and accountabilities, and/or ineffective or disproportionate oversight of decision-making and/or performance.
Operations	Risks arising from inadequate, poorly designed or ineffective/inefficient internal processes resulting in fraud, error, impaired customer service (quality and/or quantity of service), non-compliance and/or poor value for money.
Legal	Risks arising from a defective transaction, a claim being made (including a defence to a claim or a counterclaim) or some other legal event occurring that results in a liability or other loss, or a failure to take appropriate measures to meet legal or regulatory requirements or to protect assets (for example, intellectual property).
Property	Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public.
Financial	Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed, and/or non-compliant financial reporting.
Commercial	Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in poor performance, inefficiency, poor value for money, fraud, and /or failure to meet business requirements/objectives.
People	Risks arising from ineffective leadership and engagement, suboptimal culture, inappropriate behaviours, the unavailability of sufficient capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies resulting in negative impact on performance.
Technology	Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience.
Information	Risks arising from a failure to produce robust, suitable and appropriate data/information and to exploit data/information to its full potential.
Security	Risks arising from a failure to prevent unauthorised and/or inappropriate access to the estate and information, including cyber security and non-compliance with General Data Protection Regulation requirements.
Project / Programme	Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits to time, cost and quality.
Reputational	Risks arising from adverse events, including ethical violations, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations.

Failure to manage risks in any of these categories may lead to financial, reputational, legal, regulatory, safety, security, environmental, employee, customer and operational consequences.

Ref:		Risk Register:		Risk Owner:	

Objective:		Risk:		Potential Consequences:	

Current Mitigations	Risk Causes	MITIGATIONS How risk is currently managed	Evidence to assess effectiveness and date of last review	Officer responsible

Additional Actions	Additional ACTIONS	Responsibility	Due date	Current status / comments

Overall Assessment	Impact	Likelihood
Inherent Risk		

Mitigations

Residual Risk		

Further Action

Target Risk		

Risk Appetite	

Qualitative Measures of Impact

Impact	Score	*Description and Action Needed*	*Impact on individual(s) – staff or public.*	*Statutory Duty.*	*Business / Operational*	*Buildings/ Engineering/ Environmental*	*Quality of Service*	*Finance*
Catastrophic (Very High)	5	*This is above the Council's defined tolerance level. Comprehensive action required immediately to mitigate the risk.*	• *Death*	• *Multiple breach of statutory legislation and prosecution.*	• *Litigation > £500k expected.* • *National Media Interest* • *Severe loss of confidence and reputation*	• *Critical Environmental Impact.* • *Service closed for unacceptable period.*	• *Severe impact on customer satisfaction.* • *Gross failure to meet professional / national standards*	• *Significant financial impact (over 5% of total directorate budget)* • *Theft / loss >£250k*
Major (High)	4	*Consequences are severe but not disastrous. Some immediate action may be required. Development of a comprehensive action plan may be required.*	• *Major injury/ill health (reportable)* • *Major clinical intervention* • *Permanent incapacity*	• *Multiple breach of statutory legislation and improvement notice issued.*	• *Litigation >£250k to <£500k expected.* • *Adverse publicity* • *Impact on reputation*	• *Major/significant environmental impact* • *Severe disruption to service*	• *Major impact on customer satisfaction.* • *Failure to meet professional / national standards*	• *Major financial impact (between 2% - 5% of total directorate budget.* • *Theft / loss between £100k - £250k*
Moderate (Medium)	3	*Some immediate action may be required. Development of action plan may be required. Risk status should be monitored regularly.*	• *Temporary Incapacity* • *Short term monitoring* • *Additional medical treatment up to 1 year* • *Extended hospital stay.*	• *Single breach of statutory legislation and Improvement Notice issued.*	• *Litigation >£50k - <£250k possible.* • *Potential for adverse publicity, avoidable with careful handling* • *Potential to impact on reputation.*	• *Moderate environmental impact* • *Moderate disruption to services*	• *Formal complaint expected.* • *Failure to meet internal standard*	• *Moderate financial impact (between 1% and 2% of total directorate budget)* • *Fraud/Theft / loss between £50k - £100k*
Minor (Low)	2	*No immediate action required. Action plan should be considered. Risk status to be monitored periodically.*	• *First Aid/ self treatment* • *Minor injury* • *Minor ill health up to 1 month* • *Near miss (small cluster)*	• *Breach of statutory legislation.*	• *Litigation <£50k* • *Impact on reputation – internal awareness,*	• *Localised environmental impact* • *Disruption to service perceived as inconvenient*	• *Possible complaint.* • *Single failure to meet internal standard.*	• *Minor financial impact (up to 1% of total directorate budget)* • *Fraud/Theft / loss between £1k - £50k*
Insignificant (Very Low)	1	*Risk status to be reviewed occasionally.*	• *Near miss (single)* • *No adverse outcome* • *No injury or ill health*	• *Near breach of statutory legislation.* • *Minor breach of guidance or legislation.*	• *Possible litigation due to settlement is <£5k.*	• *Minimal impact to environment.* • *Minimal disruption.*	• *Customer initially unhappy.* • *Minor non-compliance with internal standard.*	• *Theft / loss up to £1k.*

Qualitative Measures of Likelihood

Likelihood of Event or Incident occurring		
Likelihood Descriptor	**Score**	**Probability / Likelihood** (of event or incident occurring over lifetime of Corporate Plan).
Almost Certain	**5**	• The event is more likely than not to occur.
Likely	**4**	• The event is likely to occur.
Possible	**3**	• There is a reasonable chance of the event occurring.
Unlikely	**2**	• The event is unlikely to occur.
Rare	**1**	• The event will occur only in exceptional circumstances.