APPENDIX B

CAERPHILLY COUNTY BOROUGH COUNCIL

RISK MANAGEMENT GUIDANCE

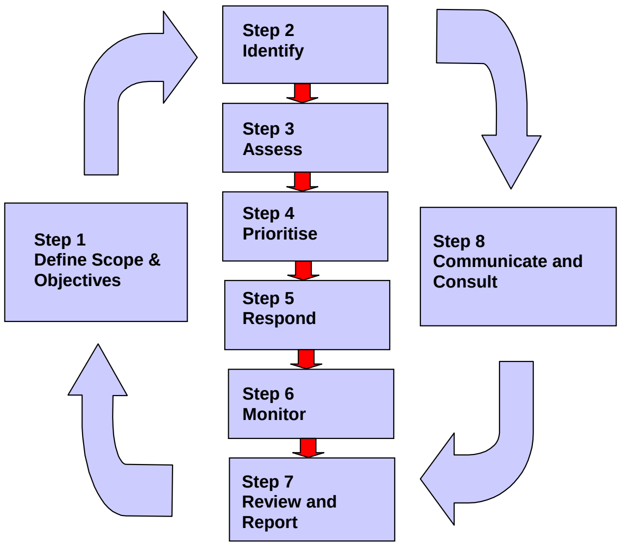
Implementing Risk Management
This guidance document accompanies the Council's Risk Management Strategy and the current Service Improvement Guidance, so reference should be made to all documents.

The purpose of this document is to improve the management of risk and provide a consistent approach across the Council.

The Risk Management Process
The process for identifying, assessing, managing and monitoring risk is an integral part of the management process. The continual identification and assessment of risk is key to the successful delivery of our outcomes.

The changing external environment and the decisions made in the course of running the Council will continuously alter the status of risks identified and new risks emerging. The risk assessment process should support this on-going and forward-looking identification and assessment of risk as part of running the Council.

An overview of the risk assessment process is shown below:



The risk register is how risks are documented. The current risk register format is included in Appendix 1. Its purpose is to provide a consistent method for capturing risk information. While it should be used at all steps in the process, it is important to make it a relevant and dynamic document. Its main purpose is to help ensure we <u>take action</u> where we need to.

The Corporate Risk Register documents the risks to the Council as a whole. In addition, each Service and Partnership is required to maintain an up-to-date risk register. It is left to the Service to decide whether it also records its risk assessment and maintains risk registers at business unit level. This will depend on the size, complexity and range of activities in the service. Project risks should be identified during the PID stage and, where a project progresses, the Project Manager is required to maintain an up-to-date risk register for that project.

Risk assessment will not be relevant or dynamic if we just go through the motions of writing down lists of risks.

Risk assessments, at all levels, are carried out within the regular business planning cycle, making risk management part of an established process, and ensures that the mitigation actions for key risks are included within business plans. As risk management is integrated with business planning, the existing performance management system is used to measure risk management performance.

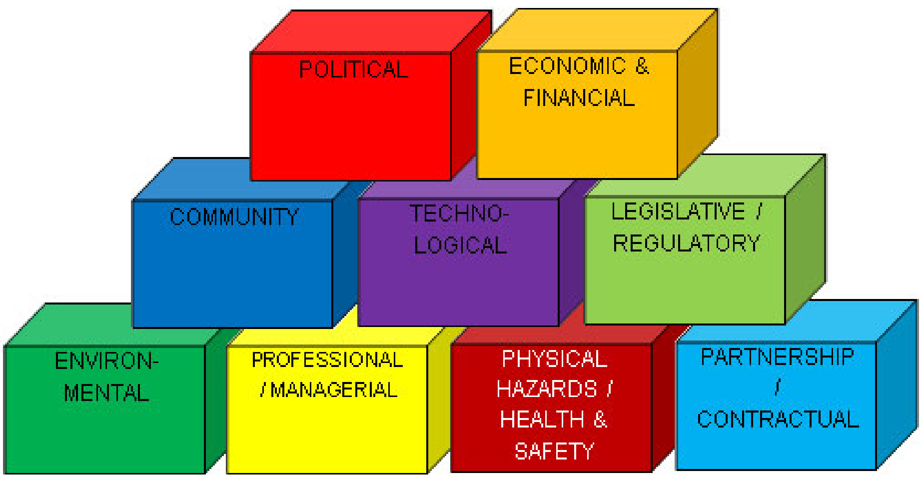
Stage 1 – Define Objectives
It is important that those involved in the risk assessment process clearly understand the relevant key business objectives i.e. *'what we want to achieve'* in order to be able to identify *'the barriers to achievement'*. The more clearly objectives are defined, the easier it will be to consider those risks that could actually impact on objectives. Objectives must therefore be SMART (Specific, Measurable, Agreed, Realistic and Time bound). It follows therefore that:-

- Corporate and strategic risks are identified and prioritised in relation to the Council's Vision and key objectives;
- Directorate and Service risks are identified and prioritised in relation to the service business plan;
- Partnership and project risks are identified and prioritised in relation to the particular objectives of the partnership / project.

Stage 2 – Risk Identification
Risk identification attempts to identify the Council's exposure to uncertainty. To ensure that key risks are identified, the process requires imagination, creativity, ingenuity and wide involvement as well as a methodical framework.

This is probably one of the most important steps of the process, as we can only attempt to manage risks we have identified.

To try and achieve a robust risk assessment, it is useful to consider the whole spectrum of risk, which is all of the various areas where the Council or service may face risk. The following categories may be used as prompts to aid the thought process:



These are explained in more detail within Appendix 2 (which gives examples but is not an exhaustive list). Using the prompts, various techniques can be used to begin to identify risks including:-

- Brainstorming;
- Past experience;
- ‘Strengths, Weakness, Opportunities and Threats’ analysis or similar;
- Exchange of information/best practice with others.

No one person holds all the risks, so to ensure that the process is as comprehensive as possible a group should identify the risks whatever method(s) are used.

It is important to also identify those risks where their contribution to objectives are not totally clear, particularly at operational or service levels where risks to safety and financial loss should also be considered, as should risks around compliance and statutory requirements.

Risks should be captured whether they are under the Council’s direct control or not. For significant partnerships, the risks to the Council as well as the risks to the partnership itself need to be considered.

Finding the right words which is explained in the SIP guidance, to properly define a risk is important in order that it is clear what the risk is. A good guide is that we must be able to look back and say whether the risk event has occurred or not. It is advisable to start a description with “The risk that…”, or “The risk of……”. Only using a short phrase normally leaves too much room for different interpretation, e.g. “IT failure” compared to “The risk that failure of the xxx system results in significant disruption to service provision”. Once risk is identified, one of the most effective questions is “what happens now?”.

Stage 3 – Assess

Having identified a risk (or vulnerability) it is important to assess the causes or triggers, the potential consequences/impact and how effectively it is being managed. It is the management of the cause(s) and consequence(s) that determines how well a risk is controlled. This, in turn, determines what further actions may be necessary.

The vulnerability is essentially the risk, or the weakness that currently exists. The triggers are what are or could cause the risk to materialise, whilst the consequences are the ‘worst likely’ chain of events that could occur were the trigger to occur.

When assessing the risk impact and likelihood we do so on a residual basis. The residual risk is the risk as it currently stands with existing controls in place.

Stage 4 – Prioritise Risks

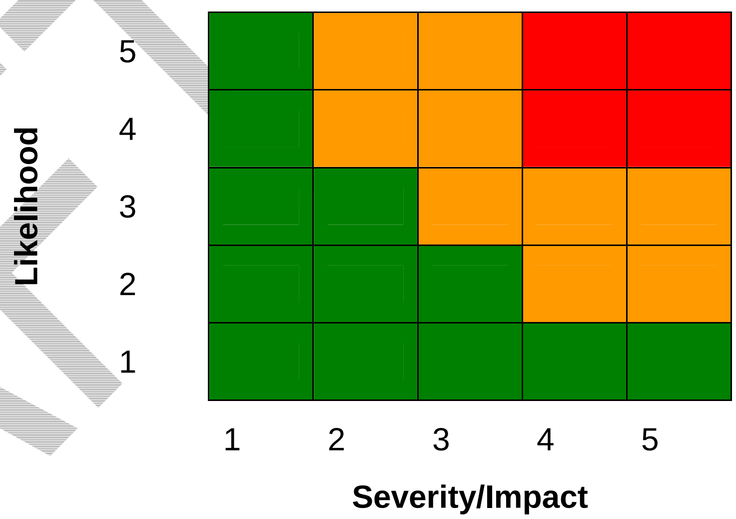
As there is finite time and resources available, not all identified risks can be managed, so following identification and analysis the risks will need to be evaluated to assess the really key ones. The likelihood and severity or impact of each risk is, therefore, assessed within the relevant timeframe of the business plan/project.

Likelihood is assessed by asking how likely it is that the trigger event should occur in the given timeframe.

The potential impact or severity of the risks, or more specifically the identified consequences, should be compared to the appropriate objectives. The challenge for each risk is how much impact it could have or is having on the ability to achieve the objectives.

Appendix 3 provides a risk assessment criteria for corporate risks. The risk assessment criteria used are "semi-quantitative" which allows the assessment to be more objective and enables risks to be prioritised and escalated consistently. The risk assessment criteria can be used as a guide for Service, Project, and Partnership risks but will need to be scaled in relation to size, budget and prominence of the Service, Project or Partnership concerned. To give some guidance, a likelihood of 5 could be said to be "something that is already occurring, or certain to occur", the other categories, therefore, scale down. On severity 5 it could be said "the impact is such that all, or a substantial number, of the relevant objectives cannot be achieved" and the others scale down. It is important when scoring the likelihood and impact of risks that a balanced view is taken.

The combination of likelihood and severity/impact provides a risk score allowing risks to be plotted on the matrix and set the risks in perspective against each other.



Likelihood

1 Rare
2 Unlikely
3 Possible / Moderate
4 Likely
5 Almost Certain

Severity

1 Insignificant
2 Minor
3 Moderate
4 Major
5 Catastrophic

Those risks towards the top right hand corner with higher likelihoods and impacts (red) are the most pressing with the priority falling as we move down to the bottom left hand corner.

This prioritisation helps us decide where to focus our risk management efforts. Those risks in the green blocks should not be ignored but no significant effort or resource will be used to manage them.

Stage 5 – Respond To Risks

This is vitally important as it is during this stage that improvement actually occurs. There are normally options for improving the management of a risk and they fall into the following categories. Currently the SIP guidance has similar categories.

Response	Which means?	Example
Tolerate	Do nothing 'extra' to manage the risk	Where current control measures are sufficient to reduce the likelihood and impact of risk to a tolerable level that there is no added value in doing more, or not cost effective or realistic to try and manage it further. Where risks that are outside of our control and we have no influence over them e.g. Government introducing legislation that has a negative impact on the Council. These risks have to be accepted, but can be monitored.

Treat	Mitigating the risk by managing: • the likelihood • the impact • or both	The most likely form of management for the majority of risks. Developing SMART actions to manage the likelihood of risks occurring, their impact if they were to occur, or both. Preventative controls are used to mitigate likelihood – to ensure something does not happen e.g. training so that staffs do not do something in the wrong way or firewalls to prevent computer virus attack. Impact is often mitigated with some kind of contingency e.g. alternative service providers or alternative service arrangements.
Transfer	Insurance / outsourcing / partnerships	Insurance, although will not be applicable for most of the risks faced. Outsourcing or entering into partnerships may transfer certain risks, however, will inevitably create new and different risks which have to be managed.
Terminate	Stop doing an activity	Where a risk could be so serious that there is no other option but to terminate the activity that is generating the risk. This can be difficult for a local authority given the number of statutory functions, however, non-statutory services could cease.

Where required, specific actions should be developed with defined ownership and timescales. When the risk assessment is conducted alongside the business planning process, actions should be integrated in the business plan.

In determining what actions are required, it is important to consider the effect these will have on controlling the risk in question, and specifically what change they will make to the impact and/or likelihood of the risk. Consideration should also be given here as to the 'Cost-Benefit' of each control weighed against the potential cost/impact of the risk occurring. N.B. 'cost/impact' here includes all aspects including financial, resourcing, but also reputational.

Stage 6 – Monitor Risks

The monitoring of risks is a normal management activity and as such should be integrated as part of normal line management responsibilities. Risk Management is not a one off exercise – it needs to be an integral part of the way we work. Progress in managing risks will be monitored and reported so that losses are minimised and intended objectives are achieved.

Monitoring of risks and the actions identified to mitigate them is, therefore:

- part of existing performance monitoring timetables;
- focused on those risks that have been given the higher priority (red).

Service risks and the actions identified to mitigate them will be formally monitored and reviewed as part of the quarterly Service Performance Reviews.

Stage 7/8 – Review And Report / Communicate And Consult

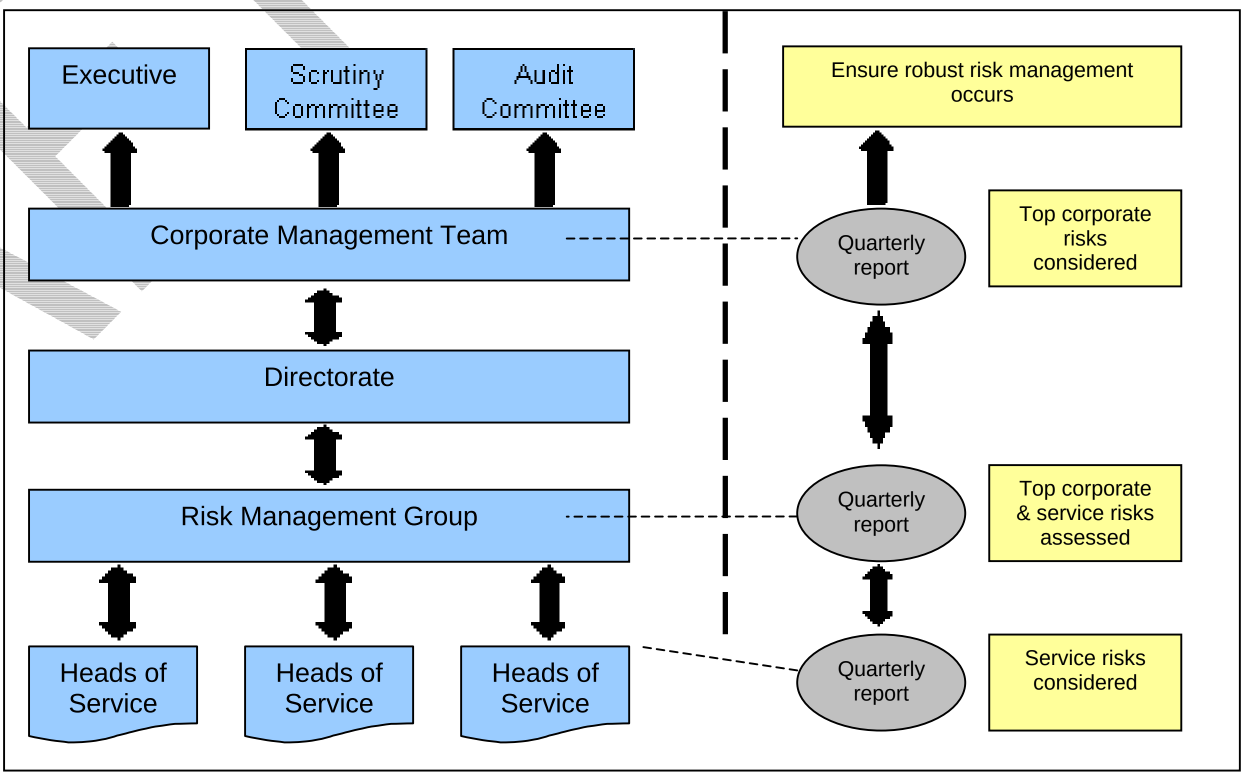
The annual planning process is the point at which outcomes are reviewed and revised and is, therefore, a logical point at which to also review key risks and how they are managed. Business planning presents the opportunity to be forward looking and pro-active in our management of risk. Within the planning process (e.g. business cases, service plans) it is necessary to answer three main questions:

- Have we considered what we need to do in the year(s) ahead to deliver our plans, and the risks of not doing these things?
- Have we considered what might go wrong, with significant impact, in our plan, and how we would spot it in a timely manner?
- Have we considered external risks and identified those it is realistic for us to plan for?

Discussion, review and reporting of risk should take place at regular management and team meetings. Key risks and action progress should be reviewed at these meetings as determined by the severity of the risk.

Regular internal reports enable senior managers and Members to be fully aware of the extent of the risks and the changes occurring to them. In practice, risks will be reported as part of the performance management and business planning processes.

Internal reporting arrangements provide different levels of the Council with the most appropriate information. The reporting process is explained in detail in the Risk Management Strategy but is summarised below:



The Risk Management Group will act as "gatekeeper" for those risks being pushed up from Service Risk Registers to the Corporate Risk Register and risks pushed down from the Corporate Risk Register to Service Risk Registers. This will ensure consistency and identify common themes.

New risks identified should be added to the relevant risk register as soon as they have been identified. Where this is a significant (red) risk it must be reported on an exception basis through the relevant management structure and not left until the next routine round of reporting.

The likelihood and impact of each risk must be regularly reviewed in the light of the effects of control measures or other factors affecting the risk. Where the control measures are successful the risk score should reduce but where the control measures are ineffective or inadequate the risk score could increase. Under such circumstances the existing mitigation action must be reviewed and consideration given to introducing additional control measures.

Where a previously identified risk is no longer a risk to the objectives, consideration should be given to removing the risk from the relevant risk register. This should only be done once the risk has been sufficiently scrutinised as part of the relevant performance management review.

All aspects of the risk management process will reviewed at least once a year.

Appendix 1 – Risk Register

Ref	Aspect	Risk Description	Risk Level 2012-13 (Aug 2012)	Risk Level 2013-14 (Feb 2013)	Risk Level 2013-14 (Aug 2013)	What has been done to mitigate the risk?	Risk Owner
			Medium	Medium			
			High	High			
			Low	Medium			
			Medium	Medium			
			Low	Low			
			Low	Low			
			High	High			
			High	High			

Appendix 2 – Categories of Risk

Political Arising from the political situation • Change of Government Policy • Political make-up • Election cycles • Decision-making structure • Abuse (e.g. fraud, corruption) • Reputation management	**Economic & Financial** Arising from the economic situation and the financial planning framework • Treasury – investment, reforms • Demand predictions • Competition and the effect on price • General/regional economic situation • Value/cost of capital assets	**Community** Demographics, social trends and meeting customer needs or expectations • Residential patterns and profile • Social care • Regeneration • Customer care • Quality of community consultation
Technological Arising from the ability to deal with pace of change, and the technological situation • Capacity to deal with change/advance • State of architecture • Obsolescence of technology • Current performance and reliability • Security and standards • Failure of key system or project	**Legislative/Regulatory** Arising from current and potential legal changes and/or possible breaches and the organisation's regulatory information • New legislation and regulations • Exposure to regulators • Legal challenges/judicial review • Adequacy of legal support	**Environmental** Concerned with the physical environment • Type of environment (urban, rural, mixed) • Land use – green belt, brown field sites • Waste disposal and recycling issues • Impact of civil emergency (i.e. flood) • Traffic problems, planning & transport • Pollution, emissions, noise • Climate change & energy efficiency
Professional/Managerial The need to be managerially and professionally competent • Peer reviews (e.g. IDeA, consultancy) • Stability of officer structure • Competency and capacity • Management frameworks and processes • Turnover, recruitment and retention • Profession-specific issues	**Physical Hazards and Health & Safety** Physical hazards associated with people, land, buildings, vehicles and equipment • Health, safety and wellbeing of staff, partners and the community • Accident and incident record keeping • Maintenance practises • Security of staff, assets, buildings, equipment • Nature and state of asset base	**Partnership/Contractual** Partnerships, contracts and collaboration • Key partners - public, private & voluntary • Accountability frameworks and partnership boundaries • Large-scale projects with joint ventures • Outsourced services • Relationship management • Change control/exit strategies • Business continuity • Partnerships – contractual liabilities

Appendix 3 – Risk Assessment Criteria

LIKELIHOOD	Event is expected to occur or occurs regularly	Monthly or more frequently	Almost Certain	5					
	Event will probably occur	Annually	Likely	4					
	Event may occur	1 in 2 years	Possible / Moderate	3					
	Event could occur	1 in 3 years	Unlikely	2					
	Event may occur in certain circumstances	1 in 10 years	Rare	1					
					1	2	3	4	5
					Insignificant	Minor	Moderate	Major	Catastrophic
		Service / Operations			No impact to service quality, limited disruption to operations	Minor impact on service quality, minor service standards are not met, short term disruption to operations	Significant fall in service quality, serious disruption to service standards	Major impact to service quality, multiple service standards not met, long term disruption to operations	Catastrophic fall in service quality and key service standards are not met, long term catastrophic interruption to operations
		Reputation			Public concern restricted to local complaints	Minor adverse local / public / media attention and complaints	Adverse regional or national media public attention	Serious negative regional or national criticism	Prolonged regional & national condemnation
		Financial	Cost (£)		< £50k	£50k - £350k	£350k - £1m	£1m - £5m	>£5m
					SEVERITY/IMPACT				