

<b>ISLE OF ANGLESEY COUNTY COUNCIL</b>	
<b>COMMITTEE:</b>	<b>AUDIT AND GOVERNANCE</b>
<b>DATE:</b>	<b>5 DECEMBER 2017</b>
<b>TITLE OF REPORT:</b>	<b>REVIEW OF RISK MANAGEMENT STRATEGY AND FRAMEWORK</b>
<b>HEAD OF SERVICE:</b>	<b>Marc Jones, Head of Function (Resources) / Section Officer</b> 01248 752601 <a href="mailto:MarcJones@ynysmon.gov.uk">MarcJones@ynysmon.gov.uk</a>
<b>REPORT AUTHOR:</b> TEL: E-MAIL:	<b>Julie Jones, Risk and Insurance Manager</b> 01248 752609 <a href="mailto:juliejones@ynysmon.gov.uk">juliejones@ynysmon.gov.uk</a>
<p><b>Nature and Reason for Reporting:</b> The Audit and Governance Committee's Terms of Reference require it to review the development, operation and embedding of risk management within the Council including making reports and recommendations to the Council on the adequacy of those arrangements. In addition, the Council's Risk Management policy requires the Audit and Governance Committee to review the appropriateness of its risk management and assurance processes. This report provides a review of the processes for the Audit and Governance Committee to consider.</p>	

## Introduction

1. The Council's Executive approved the Risk Management Policy in May 2015. The policy identifies that the Audit and Governance Committee has a responsibility for reviewing the appropriateness of the risk management and assurance processes in place. Together with the associated Risk Management Guidance, the policy forms the basis of the Council's approach to managing risks. These documents are appended to this report for information.

## Review of the Risk Management Strategy and Framework

2. It is prudent to review the appropriateness of these documents periodically in order to provide this Committee with an overview of the appropriateness of the risk management process. The Head of Audit & Risk and Risk & Insurance Manager undertook a review during quarter 2, in conjunction with the SLT and Penaethiaid.
3. The review found the process itself to be standard and in line with those of other organisations. It did however appear that the processes were not fully embedded into the Council's working practices, resulting in the process being a tick-box paper exercise as opposed to an essential tool for effective and informed decision-making.
4. According to the established processes, each Service is required to review and submit their service risk registers quarterly. Any red or amber risks are then referred to SLT so that they can be considered for inclusion on the Corporate Risk Register. Services were also asked for an update on any mitigating actions which need to be implemented in order to control corporate risks. The review found that not all services were presenting these updates, and that information which was submitted added little value and was often out of date. To improve this situation it has been agreed that responsibility for requesting updates and Service risk registers passes from the Performance Team to the Risk & Insurance Manager and that the Risk & Insurance Manager also meets with each Head of Service at least every six months to discuss their risks.

5. The review found that a procedure had been established for the SLT to review the Corporate Risk Register quarterly in accordance with the Risk Management Policy and Guidance. Whilst this procedure had been implemented, it had slipped for a period which meant that the SLT had not reviewed the Corporate Risk Register during the first half of 2017. In order for risk management to become fully embedded, SLT should consider any risks associated with each issue presented to them and ensure that these are captured in the relevant risk register (corporate, service, partnership or project). To address this, SLT have agreed that the Risk & Insurance Manager should attend SLT at least once every three months to assist them in reviewing the Corporate Risk Register. This will allow the Risk & Insurance Manager to present the Corporate Risk Register to this Committee and the Executive / SLT Business Meeting twice a year.
6. The review also found that Members and Officers are not always fully informed of the risks involved when taking decisions. This is because the section on Standard committee report template to note risks is rarely completed and there is no mechanism for these to be commented on or considered for inclusion on the appropriate risk register. During discussions with SLT, it was felt that a review of the committee report template was required to consider this and other issues. In the meantime, guidelines are being prepared on what should be included in the Risk section.
7. Finally, the review noted that although senior and middle managers had received training on risk management in 2014, no training had been offered to elected Members. Arrangements are therefore being made to provide training for elected Members. Similarly, Heads of Service have been asked to comment on the type of training that would benefit them and their managers in order that suitable training can be delivered.
8. Since the review, the actions noted in paragraphs 5 and 6 above have been implemented. Each Service presented an updated Service Risk Register at the end of quarter 2, which allowed an updated Corporate Risk Register to be presented to and discussed at SLT on 6 November 2017. The Risk & Insurance Manager has also met with three Heads of Service or attended their management teams to discuss their risks, with arrangements in hand to meet with two further heads of Service and their management teams before Christmas.

## **Recommendation**

9. The Committee is requested to note the content of this report and take assurance that although there remains work to be done to fully embed risk management throughout the Council, progress has been made and is continuing.

# Risk Management Policy

## Context

The Isle of Anglesey County Council is a diverse organisation committed to providing quality, sustainable and value for money services to the community. By providing strong community leadership and working in partnership, the Council is committed to realising the vision of our community strategy and Corporate Plan.

Risk is defined as *“an event that, should it occur, would impact our ability to successfully achieve our objectives”*. The Council recognises that there are risks involved in all our activities and that we have a duty to manage these risks in a balanced, structured and cost effective way. The process for identifying, assessing, managing and monitoring risk is, therefore, considered an integral part of the management process. As a result, we will be in a stronger position to enhance our service delivery capabilities, achieve our objectives and value for money.

## Vision

The vision for risk management is that it provides a framework to manage risk within agreed limits in order that the desired outcomes are achieved at a corporate, service and project level.

Failing to identify, assess and manage risks may result in considerable unbudgeted expenditure, damage to the Council’s reputation and community confidence.

It is recognised that some risk must be accepted in order that objectives can be achieved. The Council’s policy is, therefore, to ensure a culture of knowledgeable risk taking where it is explicit which risks the Council has chosen to accept, and those we have chosen not to accept.

## Objectives

The objectives of the Council’s risk management policy are to:

1. Develop a consistent approach to risk management across the Council.
2. Embed risk management as an integral part of the management process within the Council, and ensure clear links with Service Plans.
3. Ensure a proactive risk aware culture across all parts of the Council, where risk is taken (and not taken) knowledgeably in all major decisions and actions.
4. Maintain and improve customer confidence in our ability to deliver on our commitments.
5. Reduce the possibility of unplanned activity or financial costs, and the impact of such surprises on the Council’s reputation and ability to deliver our objectives.
6. Manage risk in accordance with best practice, statutory obligations and the Wales Programme for Improvement.
7. Work with our partners and providers to develop a common approach to achieving these risk management objectives.

## Principles

The following key principles set out how the Council will achieve our risk management objectives:

1. Risk management is a continuous process and not an event. The process for managing risk ensures that key risks are identified, evaluated, continuously monitored, and mitigated where necessary to an acceptable level.
2. The identification, assessment, management and reporting of risk information is timely, accurate, relevant and gives adequate coverage of the key risks in order to support management decision making.
3. The process for managing risk is an integral part of management and the successful completion of any activity, project or process.
4. Risk management is all encompassing but not burdensome or bureaucratic, nor adds unreasonably to the cost of running the Council.

## Roles and Responsibilities

The key roles and responsibilities are:

- *Chief Executive & SLT*  
The Chief Executive is responsible for effective management of risk across the Council, supported by the Senior Leadership Team and those officers charged with statutory responsibility for particular services. The Chief Executive and SLT are responsible for ensuring that the Corporate Risk Register is accurate and that risks are being well managed.
- *Heads of Service & Penaethiaid*  
Each Head of Service is responsible for implementing the Risk Management Policy and ensuring that service risks are well managed within their area of responsibility, and collectively the Penaethiaid are responsible for supporting the Chief Executive and SLT to manage Corporate Risks.
- *Elected Members*  
Responsible for good governance in the delivery of services to the community and overseeing that Council Officers have effective risk management arrangements in place.
- *Executive Committee*  
Responsible for approving the Council's Risk Management Policy, Risk Appetite and for overseeing the Corporate Risk Register.
- *Audit Committee*  
Responsible for reviewing the appropriateness of the risk management and assurance processes.
- *Corporate Scrutiny Committee*  
Scrutinise major critical risks.
- *All Employees*  
All employees have a duty to manage risk.

## Risk Management Procedures

Further guidance to support how this policy is implemented is provided in the Council's Risk Management Guidance.

# Risk Management Guidance

## 1. Introduction

### 1.1 Background

In its Risk Management Policy the Council recognises that there are risks involved in all our activities and that we have a duty to manage these in a balanced, structured and cost effective way. The process for managing risk is considered an integral part of our management and decision making processes, and contributes to the achievement of our objectives.

### 1.2 Purpose

The purpose of this document is to help manage risk and seek compliance with the policy statement. It is a guide to our approach to managing risk and how and where to apply it in the council.

### 1.3 Definition

**“Risk”** is the uncertainty of outcome, whether a positive opportunity or a negative threat, of actions or events. Our definition for risk is ‘an event that, should it occur, would impact our ability to successfully achieve our objectives’.

Risks are often confused with issues. An **“issue”** refers to the consequences of an event that has already occurred and management mitigation actions are underway or planned.

### 1.4 Regulatory Requirements

The Wales Programme for Improvement (WPI) 2010 requires all local authorities in Wales to secure continuous improvement by taking a more proactive role in the delivery of their functions at strategic and operational level. The production of service based Risk Registers and a Corporate Risk Register are important elements of the WPI requirements.

The council is required to publish an Annual Governance Statement which includes an assessment of the council’s risk management and internal control mechanisms and their effectiveness in practice.

## 2. Roles and responsibilities

Roles and responsibilities for risk management in the council are as below.

### 2.1 Chief Executive & Senior Leadership Team (SLT)

Under the leadership of the Chief Executive, SLT are responsible for the effective management of risk across the council. This is done through:

- Ensuring that Risk Management procedures remain fit for purpose and effectively implemented.
- Championing a culture of risk management within the council.
- Ensuring that the Corporate Risk Register is accurate and that risks are being well managed and properly considered in corporate decision making.
- Reviewing risk registers with Heads of Service as part of regular supervision meetings to ensure that the risks remain relevant, that emerging risks are identified, and that actions are completed.

## **2.2 Heads of Service & Pennaethiaid**

Each Head of Service is responsible for:

- Implementing Risk Management in their area of responsibility.
- Regularly identifying and evaluating the significant risks faced by their area of responsibility and taking action to ensure these are managed as effectively as possible.
- Monitoring and escalating information in a timely manner.

Collectively the Pennaethiaid are responsible for supporting the Chief Executive and SLT to manage Corporate Risks.

## **2.3 Elected Members**

All Members have a responsibility to:

- Good governance in the delivery of services to the local community and therefore overseeing that council officers follow an effective risk management process in place;
- Ensure that risks are considered as part of the decision making process;
- Understanding the corporate risks that the council faces, and being aware of how these risks are being managed;
- Raising risks not already identified (for the attention of the officers)

In addition Members who sit on the Executive, Audit, and Corporate Scrutiny Committees have the following specific responsibilities:-

### **2.3.1 Executive Committee**

- Hold the Chief Executive and SLT to account for implementing effective fit for purpose procedures to manage risk;
- Approve the Risk Management Policy and Risk Appetite;
- Oversee the Corporate Risk Register, ensuring that it is accurate and that risks are being managed effectively;
- Ensure that adequate resources are available to manage risk.

### **2.3.2 Audit Committee**

Responsible for reviewing the appropriateness of the risk management and assurance processes which are in place. To do this it will:

- Review and endorse the Risk Management Policy and Guidance
- Monitor and comment on the management and control of the Corporate Risk Register.

### **2.3.3 Corporate Scrutiny Committee**

- Major critical risks within the portfolio of Executive Members
- Ensuring that any associated risks have been considered when scrutinising decisions taken by the Executive.

## **2.4 Corporate Planning and Performance Management Team**

The Corporate Planning and Performance Management Team will support services in the effective implementation of the risk management process. The team ensures that identified risks are being appropriately addressed by the implementation of effective measures to mitigate risks incorporating principles of performance management and internal control.

## **2.5 Risk & Insurance Manager**

- Ensure that an appropriate risk management framework is in place, which is fit for purpose and is implemented consistently across the council.

- Responsible for the ongoing development and co-ordination of this risk management framework, and for the consolidation of risk management information for reporting purposes.

## 2.6 Internal Audit

The Internal Audit function provides independent assurance on the effectiveness of the internal control procedures and mechanisms in place to mitigate risks across the council. It also offers independent challenge to ensure the principles and requirements of managing risk are consistently adopted throughout the council. Internal Audit will use information from the risk management framework to inform their risk-based audit plan.

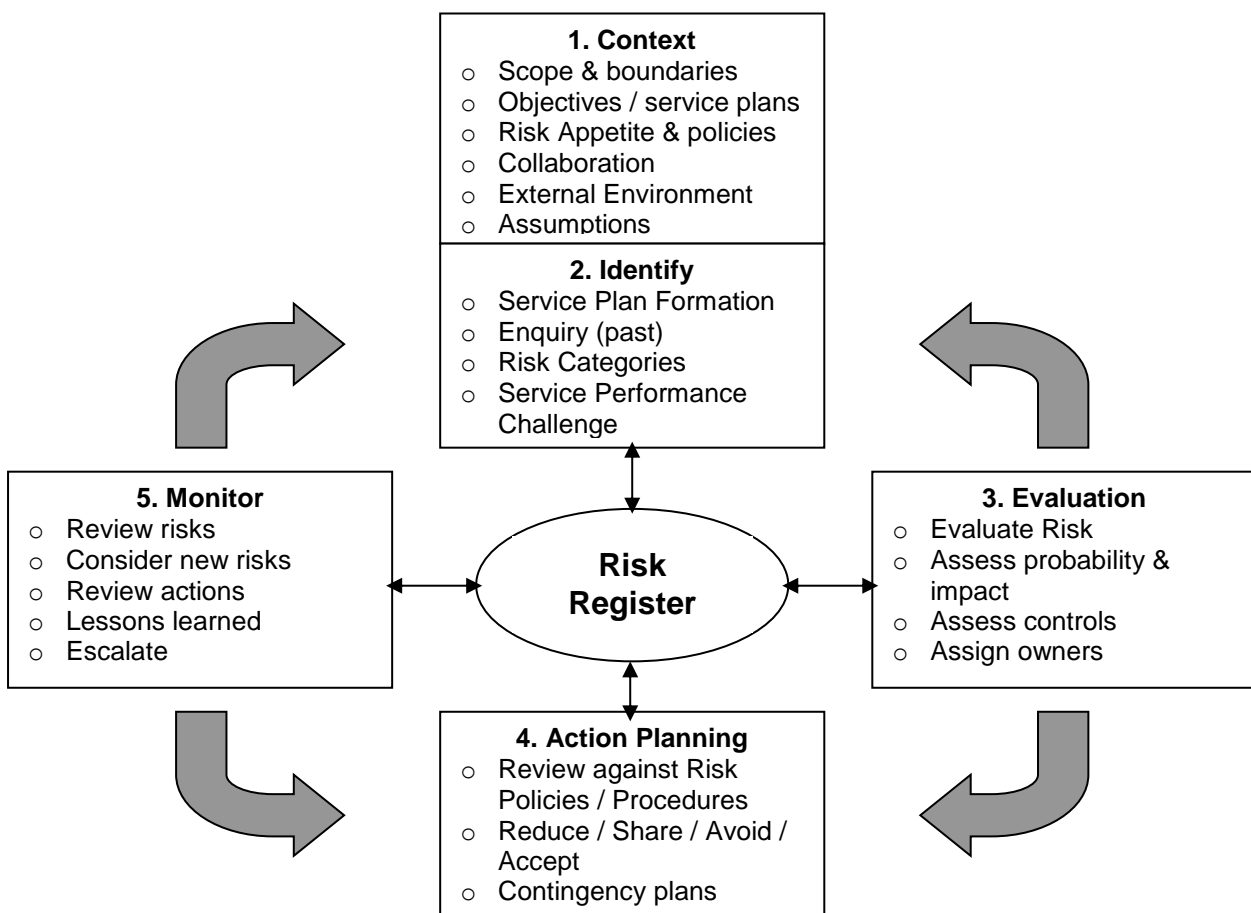
## 2.7 All staff

All staff have a responsibility for identifying risks as well as opportunities in performing their day to day duties and taking appropriate action to both manage risk, or ensure that a responsible person is made aware.

## 3. The Risk Assessment Process

The process for identifying, assessing, managing and monitoring risk is an integral part of the management process. Key to the successful delivery of our objectives is the continual identification and assessment of risk and appropriate mitigating actions are. The changing external environment and the decisions made in the course of running the council will continuously alter the status of identified risks and new risks emerging. Figure 1 shows an overview of the risk assessment process.

**Figure 1 – Risk Assessment Process**



The risk register (appendix 5) is how we document our risks. Its purpose is to provide a consistent method for capturing risk information. Its main purpose is to help ensure we take action where we need to.

### 3.1 Context

The first step is to review the context to ensure that all relevant information is considered. The following should be considered:

- Scope of the activities to be assessed (e.g. corporate, service, collaboration or project) and the associated objectives or goals (e.g. corporate plans, service delivery plan, terms of reference and project objectives).
- Impact of the changing environment, both external and internal. Externally may include political, regulatory, economic, legislative and community changes. Internally may include changing a process, service expectations, capabilities or partners.
- The level of risk the council is prepared to take in relation to the activities in question.

<b>Action Required</b>
<ul style="list-style-type: none"><li>• When reviewing their risks each service (corporate or other area) should review the context for the risk assessment. This should be done in accordance with the Corporate Planning &amp; Performance Management Framework and when major changes take place.</li><li>• Before conducting a project risk assessment the context should be reviewed.</li></ul>

### 3.2 Identifying Risks

Having reviewed the context, risks need to be identified. All risks which impact on the objectives in question should be captured, whether they are under the Council’s control or not. Opportunity is a positive side to risk that should not be overlooked and can be captured as a potential missed opportunity. All identified risks should be recorded on the relevant risk register, assigned a unique reference, and a risk owner.

There are many ways to identify risks including workshops to brainstorm ideas, individual or small meetings, looking at past experience and records.

Finding the right words to properly define a risk is important in order that it is clear what the risk is. A good guide is that we can 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...” and not use a short phrase which could be open to interpretation, e.g. “The risk that failure of the XXX IT system results in significant disruption to service provision” as opposed to “IT failure”. Objective should not be rewritten to make them a risk and issues should not be included in the risk register.

To ensure that a consistent, holistic approach is taken across the council a framework of risk categories is used (see appendix 2). This provides a common language to help the review, analysis and consolidation of risk information across the council. The risk categories are also a useful aide memoir for informing risk identification (e.g. are there areas in the categories that have not been considered?)

<b>Action Required</b>
<ul style="list-style-type: none"><li>• All identified risks should be assigned an owner, a unique reference number, and recorded on the relevant risk register.</li></ul>

### 3.3 Risk Evaluation

Having identified a risk we need to assess the causes, the potential consequences / impact and how effectively it is being managed. The causes determine the likelihood,



whilst the consequences determine the impact. It is the management of the cause(s) and consequence(s) that determines how well a risk is controlled (control effectiveness). This in turn determines what further actions may be necessary.

### 3.3.1 Risk Measurement

Risk is measured in terms of impact and likelihood against agreed criteria. The criteria we use are 'semi-quantitative', which means they are more than a simple high, medium and low approach. This provides a more objective assessment and allows risks to be both prioritised and escalated consistently. Prioritisation helps us decide where to focus our risk management efforts.

The impact of a risk is measured in five broad bands, from insignificant to catastrophic and the likelihood from rare to almost certain. When assessing likelihood it should be based on an appropriate time frame, generally over the Service Delivery Plan period but extending in line with longer-term plans if necessary. For projects the project timeframe should be used.

The combination of impact and likelihood results in a **risk exposure** rating of critical, major, moderate or minor. It is this exposure level that tells us whether or not we need to take further action or need to escalate the risk.

<b>Action Required</b>	
<ul style="list-style-type: none"> <li>All identified risks should be measured by impact and likelihood.</li> </ul>	

The risk assessment criteria used are shown in figure 2 below (see appendix 3). A slightly different set of risk assessment criteria are used for Projects and these are outlined in Appendix 4.

**Figure 2 – Risk Assessment Criteria**

LIKELIHOOD	Event is almost certain to occur in most circumstances	>70%	Almost Certain	A						
	Event likely to occur in most circumstances	30-70%	Likely	B						
	Event will possibly occur at some time	10-30%	Possible / Moderate	C						
	Event unlikely and may occur at some time	1-10%	Unlikely	D						
	Event rare and may occur only in exceptional circumstances	<1%	Rare	E						
					5	4	3	2	1	
					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		Significant impact on 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		Serious adverse local or minor adverse regional or national media public attention		Serious negative regional or national criticism		Prolonged regional & national condemnation
Financial Cost (£)		< £50k		£50k - £250k		£250k - £750k		£750k - £3m		>£3m
					IMPACT					

**Corporate Risk Severity Key**

	Minor	Risk easily managed locally – no need to involve management
	Moderate	Risk containable at service level – senior management and SLT may need to be kept informed
	Major	Intervention by SLT and / or Executive Committee involvement
	Critical	Significant SLT and Executive Committee intervention

The financial impact descriptors are set at a corporate level of materiality as appropriate. It is recognised that in each service the materiality may be lower than at a corporate level, however a single corporate set of criteria are used.

A number of different descriptors are provided to help estimate the risk impact – service / operations, reputation and financial cost. The purpose of multiple descriptors is that whilst it is not always easy to estimate the risk impact quantitatively, it is sometimes possible to compare to a qualitative statement (e.g. “regional or national media public criticism”).

In addition to the qualitative likelihood descriptors some guidance probabilities are given, these can be also considered as frequency of occurrence where 1% is equivalent to the likelihood of a 1 in a 100 year event occurring in the next year, 10% is a 1 in 10 year event, and 50% is a 1 in 2 year event, etc.

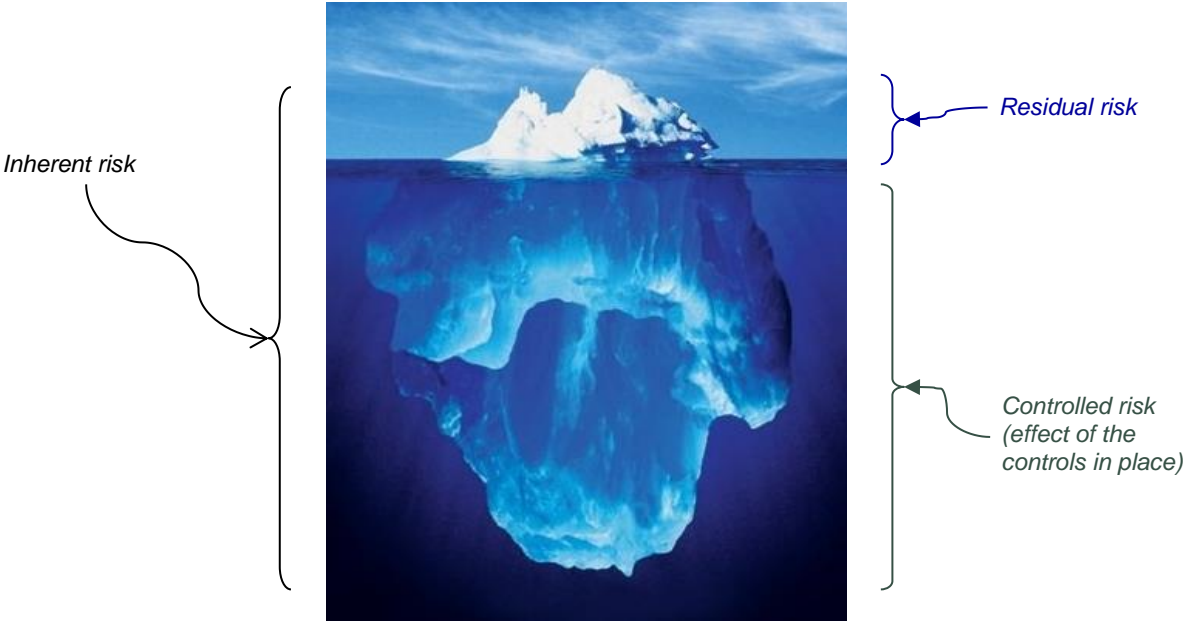
These are to be used as a guide and to provide consistency – they are not meant to be exact descriptors. If the impact of the risk falls into the 3 impact criteria, score using the highest of the three.

### 3.3.2 Inherent and Residual Risk

The risk impact and likelihood are both assessed on an inherent and a residual basis. **Inherent Risk** is the score given to the risk ignoring the effect of or considering a major failure of existing controls and before any actions to mitigate the risk have been put in place. **Residual Risk** is the risk as it currently stands with existing controls in place.

Although the residual risk may be low, the inherent risk could be high because of the importance of the controls in place to manage the risk. The relationship between the inherent and residual risk is represented in the inherent risk iceberg below.

Figure 3 – Inherent Risk Iceberg



- | Action Required   |
|---|
| <ul style="list-style-type: none"><li>All identified risks should be measured on an inherent as well as residual basis.</li></ul> |

### 3.3.3 Controls Evaluation

In assessing residual risk existing controls are taken into consideration. Existing controls are those controls already in place not those we plan to put in place. The effectiveness of each control in managing the risk, in terms of design and operating effectiveness need to be considered. Design effectiveness refers to how well the control is designed to manage the risk, while operating effectiveness refers to how well a control operates against this design. If a control is assessed as being less or more effective than it actually is then the residual risk will have been over or under estimated.

#### **Action Required**

- For the controls identified consider their effectiveness in managing the risk, and ensure that the risk impact and likelihood properly reflects this.

### **3.4 Action Planning**

A major purpose of risk assessment is to determine the need for, and extent of, any further control measures needed to mitigate the risk identified. Generally where the residual risk exposure is 'critical' or 'high' then further action is necessary. Where the exposure is 'moderate' careful consideration should be given to need for and extent of any further mitigating actions. Where no further mitigating action is not needed the rationale for this should be documented. Given that our objective is not to eliminate all risk from the organisation, then generally 'low' risks do not automatically require further action, and there may be occasions where it is appropriate to consider taking more risk.

Actions should be developed with defined ownership and timescales. When the risk assessment is conducted alongside the business planning process actions should be integrated into the Service Delivery Plan.

There are normally four options for improving the management of a risk and they fall into the following categories:

#### **3.4.1 Tolerate**

There will be some risks where the current control measures in place are sufficient to reduce the likelihood and impact of risk (residual) to a tolerable level, and that there is no need to do more or it is not cost effective to try and manage it any further.

#### **3.4.2 Treat**

The most frequent course of action will be to treat the risk, to take actions to reduce the likelihood or impact of the risk or both. Addressing the cause of a risk generally affects the likelihood (e.g. preventative measures such as improved training). Addressing the consequences generally affects the extent of the potential impact (e.g. contingency plans for alternative service providers).

#### **3.4.3 Transfer**

This involves transferring or sharing the risk with another party through such actions as outsourcing or insurance. There is normally some financial cost / benefit associated with this (e.g. premiums for insurance). Outsourcing or entering into partnerships may allow certain risks to be transferred but will inevitably bring new and different risks which have to be managed.

#### **3.4.4 Terminate**

In some instances the best alternative option is to terminate the activity that is generating the risk. In practice this can be difficult for the council given the number of statutory functions we undertake. However many authorities have stopped providing a non-statutory service due to the risks surrounding their operation.

#### Action Required

- Determine whether further action is necessary, design it and allocate owner and timeframe.

### 3.5 Monitoring

The monitoring of risks is a normal management activity and 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 actions are achieved.

#### Action Required

- Regularly monitor risks at the relevant level depending upon their importance. The minimum requirements for reviewing risk is set out in the Corporate Planning & Performance Management Framework (see appendix 6).
- Completed Risks should be supported by evidence of completion and archived.

## 4. Risk Reporting

In addition to normal management monitoring a regular cycle of risk reporting is in place, as represented in figure 4 below.

Figure 4 – Risk reporting process



### 4.1 Reporting Arrangements

Regular internal reports will enable senior managers and Members to be fully aware of the extent of the risks and the changes occurring to them.

Internal reporting arrangements provide different levels of the council with the most appropriate information. These arrangements allow:

- Regular monitoring of the corporate and service risk identification and prioritisation process as an integral part of the existing Corporate Planning & Performance Management Framework arrangements.
- Regular reports to the Executive on the Council's corporate and strategic risks.
- Annual reports to the Audit Committee on the effectiveness of the risk management framework.
- Regular reports to Members on progress in the management of key risks, including the implementation of action plans.





The Risk & Insurance Manager will assist services to prepare service and corporate risks for consideration of inclusion within the Corporate Risk Register template. All information to be included within the template will have been monitored via the Corporate Planning & Performance Management Framework. All service risks will

have been agreed and endorsed by the relevant Portfolio Member(s). All corporate risks will have been agreed and endorsed by SLT and the Executive.

**4.1.1 Escalation**

The following escalation criteria are provided (using the risk assessment criteria) to describe required management intervention depending upon the risk exposure. These criteria are set at corporate level and are not intended to suggest that a ‘moderate’ risk (at corporate level) is not important to a particular service (at service level) and might require further actions or monitoring at that service level.

**Figure 5 – Escalation Criteria Key**

	Minor	Risk easily managed locally – no need to involve management
	Moderate	Risk containable at service level – senior management and SLT may need to be kept informed
	Major	Intervention by SLT and / or Executive Committee involvement
	Critical	Significant SLT and Executive Committee intervention

**Action Required**

- Escalate risks in accordance with the escalation criteria.
- Major or Critical Risks identified outside the normal Corporate Planning & Performance Management arrangements which need escalating should be reported to SLT via the Risk & Insurance Manager. All other risks should be reported through the normal management process.

**4.2 Risk Register**

The risk register (see appendix 5) is how we document and report risks and actions to manage them and should be kept up-to-date and regularly discussed as part of the management process.

Risks with minor inherent risks do not have to be added to the risk register as they are not of significant concern in terms of likelihood or impact. Risks with minor residual risk but moderate, major or critical inherent risk do need to be included as any failing on the effectiveness of the existing controls could be of concern.

**5. Application of the Risk Assessment Process**

**5.1 Corporate Planning & Performance**

The Corporate Planning & Performance Framework provides key periods at which we review and revise our objectives, it is therefore logical to also review our key risks and how we manage them at the same time. Risk refers to those events that may impact our ability to achieve our objectives therefore business planning presents the opportunity to be forward looking and pro-active in our risk management.

Within our planning process (e.g. business cases, service delivery plans) it is necessary to consider:

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

#### **Action Required**

- Risk assessment should be conducted as part of business planning and included in the Service Delivery Plan. Risk registers should be updated by services to reflect any changes arising from this.
- In monitoring the Service Delivery Plan during the year risks should also be reviewed.

### **5.2 Business as Usual**

The day-to-day management of risk is a line management responsibility. In practice while risk management should be applied in day-to-day decision-making there are specific times when progress against objectives and the outcome of operational decisions are reviewed. It is at these points that a formal discussion of risk should happen and at which point the risk registers should be updated to reflect this. Discussion, review and reporting of risk should take place at regular management and team meetings. Key risks and action progress are reviewed at these meetings as determined by the severity of the risk.

Each service and partnership is expected 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.

#### **Action Required**

- Service risks should be regularly reviewed as part of business as usual processes (e.g. regular management meetings) and new or emerging risks considered.
- An up-to-date Service Risk Register must be maintained by the service.
- Services can decide if business unit risk registers are needed.
- Self assess

### **5.3 Projects**

Projects have clearly defined objectives, including scope, timeline and budget and it is therefore an obvious step to identify, assess and manage risk as part of projects. The risk assessment process is essentially the same as for business as usual.

Resource invested in reducing risk in the early stages of a project is resource well invested. Risks incurred during the project have to be diagnosed and fixed, and will add to costs. The rate of increase in the cost of risk is often exponential, and risks that can be reduced or eliminated during the start-up phase will pay a generous dividend in limiting the total project cost. It is better to identify and manage risks at the start-up phase of the project than to allow a contingency on a basis that things are bound to go wrong, but we don't know what!

The financial risk assessment criteria are changed to reflect each project (see appendix 4)

#### **Action Required**

- Risk assessment should be conducted as part of all projects. Risk registers should be established at start-up and maintained through the project lifecycle;
- The effective management of project risks should be considered as part of the project post implementation reviews.

### **5.4 Partnerships**

A partnership is defined as “a joint working arrangement where the partners are otherwise independent bodies, agree to co-operate to achieve a common goal of community cohesion and to achieve it, create an organisational structure or process and agreed process”

One important aspect of governance is the management of risk and partnership working brings with it a number of risks that need to be managed. Decisions to enter into partnerships should be based on a sound understanding of the risks and challenges, as well as the anticipated benefits.

There are two aspects to risk management in partnership working:

a. Outside looking in – the risks to the Council by being part of the partnership

Risks to the Council should be identified at the inception stage and incorporated into the Partnership business case. If the Partnership proceeds then the risks identified, together with any mitigating actions, should be included in the relevant Service risk register. The responsibility for ensuring that the risk management process is followed lies with the relevant organisational managers and Portfolio Holders who’s remit the Partnership falls under.

b. On the inside – the risks to the Partnership

In order to provide members of a partnership with assurance each Partnership should establish its own arrangements for managing risk. If the lead organisation has a tried and tested risk management strategy and methodology, consideration should be given to applying this to the Partnership.

Although not a requirement, partners are encouraged to use the risk register format and Risk Assessment Criteria used by the Council.

<b>Action Required</b>
<ul style="list-style-type: none"><li>• Risks to the Council should be identified at the inception stage and incorporated into the Partnership business case.</li><li>• Risks to the Council / Service of being part of a partnership should be reflected in the Corporate / Service risk register.</li><li>• Each partnership must have their own risk register and each partner should have sight of the risk register at least once a year.</li></ul>

## Appendix 1 – Risks and Issues

Risks are often confused with issues.

**“Risk”** is ‘an event that, should it occur, would impact our ability to successfully achieve our objectives’. A risk is a potential event or future uncertainty.

An **“issue”** refers to the consequences of an event that has already occurred and management mitigation actions are underway or planned.

The difference therefore is that a risk has not happened but an issue has already happened.

Examples of risks and issues are included below:

<b>Risk</b>	<b>Issue</b>
The risk of an employee being seriously injured at work following a slip, trip or fall	The condition of the building is poor and does not make the service look professional
The risk of failure of the payroll system results in staff not being paid	There is a lack of investment in IT systems
The risk that future settlements from Welsh Government to the Council destabilise the Council’s financial standing	Budget cuts mean that current financial commitments cannot be met

Issues and objectives should not be rewritten to make them a risk.



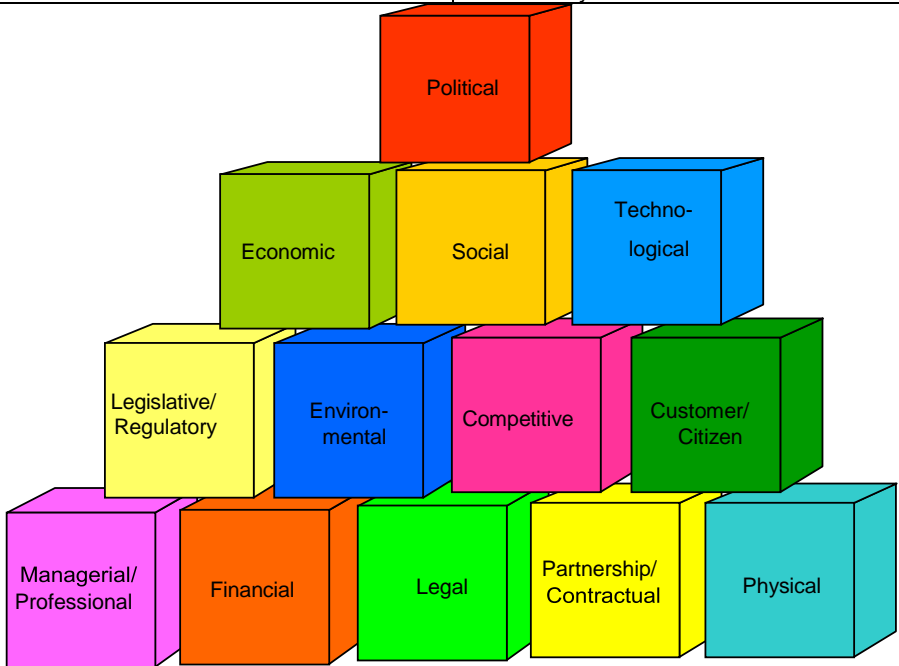
## Appendix 2 - Risk Categories

Risk categories focus on the source of risk, and are intended to be used as a set of prompts to consider scenarios that will give rise to consequences that will impact on specific objectives.

Successful risk categorisation can be compared to an effective medical evaluation. If the doctor asks: "How do you feel?" the patient might say, "Fine." But the examination is much more revealing if the doctor asks: "How do your knees feel? How about your lungs? Any back pain?" With these questions, the patient will begin to think specifically about his or her body parts.

The categories used by this Council are included in the table below, and are based on categories used by other councils; consideration of how useful each prompt will be for shaping the thoughts of those identifying risk, and practical attempts at applying these categories to the risks that services have identified.

Political	Economic	Social
<p>Arising from the political situation</p> <ul style="list-style-type: none"> <li>• Change of Government Policy</li> <li>• Delivery of Local Policy &amp; Strategic Priorities</li> <li>• Change of local policy or priorities.</li> <li>• Unfulfilled promises to electorate</li> <li>• Political make-up</li> <li>• Stability of political situation.</li> <li>• Election cycles</li> <li>• Decision-making structure</li> <li>• Meddling/abuse (fraud, corruption, lack of strategic focus)</li> <li>• Leadership issues.</li> <li>• Reputation Management</li> <li>• Response to innovation/modernisation.</li> </ul>	<p>Arising from the national, local and organisation specific economic situation</p> <ul style="list-style-type: none"> <li>• Treasury – Investments, Reforms.</li> <li>• Borrowing, lending situations, investments and interest rates.</li> <li>• Budgetary position.</li> <li>• Key employment sectors (e.g. over reliance on key employers).</li> <li>• Poverty indicators.</li> <li>• Demand predications (e.g. on demand led services like benefits, social care).</li> <li>• Competition between suppliers and the effect on service/pricing.</li> <li>• General/regional economic situation.</li> <li>• Unrecorded liabilities</li> <li>• Value/cost of capital or assets.</li> <li>• Impact of civil emergency (e.g. flood).</li> <li>• Council Tax levels</li> </ul>	<p>Arising from the national and local demographics and social trends.</p> <ul style="list-style-type: none"> <li>• Social changes – needs, expectations and attitudes</li> <li>• Demographic profile (age, race, etc).</li> <li>• Residential patterns and profile (e.g. temporal, commuter belt, state of housing stock, public/private mix).</li> <li>• Health statistics/trends.</li> <li>• Leisure and cultural provision.</li> <li>• Crime statistics/trends.</li> <li>• Children at risk.</li> <li>• Older people.</li> <li>• Employment.</li> <li>• Life-long learning.</li> <li>• Regeneration.</li> <li>• Disadvantaged groups or communities.</li> </ul>
Legislative/Regulatory	Environmental	Competitive
<p>Arising from current and potential legal changes and the organisation's regulatory information.</p> <ul style="list-style-type: none"> <li>• New legislation – National and European Law.</li> <li>• New regulations</li> <li>• Exposure to regulators – e.g. auditors/inspectors, intervention.</li> <li>• Responsiveness to criticism.</li> <li>• CPA, ESTYN, CSSIW, JAR and APA.</li> <li>• CAA – Annual Risk Assessment, Use of Resources (UoR), Direction of Travel (DoT)</li> <li>• LAA – statutory duty to cooperate, targets, performance and annual report.</li> <li>• Children's Trust</li> <li>• European Directive – Procurement</li> <li>• CCA – Emergency Preparedness, Business Continuity</li> <li>• Section 17 – Crime &amp; Disorder Act 1998</li> <li>• Equality – RRA, RED, DSA, EER, GRA</li> </ul>	<p>Arising from inherent issues concerned with the physical environmental.</p> <ul style="list-style-type: none"> <li>• Nature of environment (urban, rural, mixed).</li> <li>• Land use – green belt, brown field sites.</li> <li>• Waste disposal and recycling issues.</li> <li>• Exposure to drainage problems/flooding/erosion/subsidence/ landslip.</li> <li>• Impact of civil emergency (e.g. flood)</li> <li>• Traffic problems/congestion.</li> <li>• Planning, Transportation.</li> <li>• Pollution, emissions, noise.</li> <li>• Climate change</li> <li>• Energy efficiency</li> </ul>	<p>Arising from the organisation's competitive spirit and the competitiveness of services, etc.</p> <ul style="list-style-type: none"> <li>• Position in league tables.</li> <li>• Relationships with neighbours and partners, e.g. competitive or collaborative.</li> <li>• Plaudits held/sought, e.g. Beacon Council status.</li> <li>• Success in securing funding.</li> <li>• Nature of service provision.</li> <li>• Competition for service users. e.g. car parks.</li> <li>• Bids for Government funds.</li> <li>• Cost, quality, value for money.</li> <li>• Public against Private Sector or Other Agency.</li> </ul>

Professional/Managerial	Financial	Legal
<p>Arising from the need to be managerially and professionally competent.</p> <ul style="list-style-type: none"> <li>• Views arising from peer reviews – e.g. IdeA, consultancy reviews, internal audit, etc.</li> <li>• Professional/managerial standing of key officers.</li> <li>• Stability of officer structure/management teams.</li> <li>• Competency and capacity – Organisational and Individual.</li> <li>• Key staff changes and personalities.</li> <li>• Turnover, recruitment and retention, talent management &amp; succession planning.</li> <li>• Change – implementation and management.</li> <li>• Training and development</li> <li>• Partnership working</li> <li>• Management frameworks &amp; processes – efficient, effective.</li> <li>• Profession specific issues.</li> <li>• Mission, Vision and Values</li> </ul>	<p>Arising from the financial planning and control framework</p> <ul style="list-style-type: none"> <li>• Financial situation of authority.</li> <li>• Level of reserves.</li> <li>• Budgetary policy and control.</li> <li>• Delegation of budget and financial disciplines.</li> <li>• Monitoring and reporting systems.</li> <li>• Control weaknesses – anti fraud &amp; corruption</li> <li>• Income &amp; Revenue</li> <li>• Grants &amp; External funding</li> <li>• Insurance – adequacy of covers, level of self-funding, deductibles, etc.</li> <li>• Capital</li> <li>• Interest rates, inflation, income tax, etc.</li> <li>• Efficiency, invest in priorities, disinvestments non-priority areas.</li> </ul>	<p>Arising from changes to legislation and/or possible breaches of legislation.</p> <ul style="list-style-type: none"> <li>• Legal challenges, judicial review</li> <li>• Adequacy of legal support.</li> <li>• Boundaries of corporate &amp; personal liabilities.</li> <li>• Sufficient reserves to defend legal challenge or unrecorded liabilities.</li> <li>• Reputation Management</li> <li>• Partnerships – Legal Liabilities, contractual liabilities.</li> </ul>
Partnership/Contractual	Technological	Customer/Citizen
<p>Arising from partnerships and contracts.</p> <ul style="list-style-type: none"> <li>• Key partners – from public, private and voluntary sectors.</li> <li>• Accountability frameworks and partnership boundaries.</li> <li>• PFI schemes.</li> <li>• Large scale projects involving joint ventures.</li> <li>• Outsourced services.</li> <li>• Relationship management</li> <li>• Procurement arrangements/contract renewal policy.</li> <li>• Performance of partnerships/contractors</li> <li>• Business Continuity – Partner/Contractor arrangements.</li> <li>• Change - Change control, exit strategies.</li> <li>• Capacity and Capability – increase to deliver priorities.</li> <li>• Reputation management</li> <li>• Legal liabilities, contractual liabilities.</li> </ul>	<p>Arising from technological change and the organisational technological situation.</p> <ul style="list-style-type: none"> <li>• Technological strategy</li> <li>• Technological change/advance – capacity to deal with change/advance.</li> <li>• Current use of/reliance on technology.</li> <li>• Current or proposed technology partners.</li> <li>• State of architecture.</li> <li>• Obsolescence of technology.</li> <li>• Current performance and reliability.</li> <li>• Security and standards, e.g. back up, recovery, confidentiality.</li> <li>• Technological demand – customer needs and expectations</li> <li>• Failure of key system or key technological project.</li> <li>• Technological support for innovation.</li> <li>• Procurement of best technology and sustainability of system.</li> </ul>	<p>Arising from the need to meet current &amp; changing needs or expectations of customers and citizens.</p> <ul style="list-style-type: none"> <li>• Customer Care</li> <li>• Extent and nature of consultation with/involvement of community, e.g. community groups, local businesses, focus groups, citizens' panels, etc.</li> <li>• Demographics – analysis, understanding.</li> <li>• Relationship with community leaders, tenant groups and 'opposition' groups.</li> <li>• Visibility of services e.g. refuse collection, street cleaning, etc.</li> <li>• Service delivery – response, feedback, complaints, compliments.</li> <li>• Reputation Management – Public and media communication</li> <li>• Outcomes for area - LAA (outcomes, targets. etc).</li> <li>• Community cohesion</li> </ul>
Physical		
<p>Arising from physical hazards or possible gains associated with people, land, buildings, vehicles, plant and equipment.</p> <ul style="list-style-type: none"> <li>• Assets - Nature and state of asset base including record keeping.</li> <li>• Commitment to health, safety and wellbeing of staff, partners and the community.</li> <li>• Risk assessments.</li> <li>• Accident and incident record keeping.</li> <li>• Maintenance practices.</li> <li>• Business Continuity</li> <li>• Security – staff, assets, buildings, equipment, plant, machinery, vehicles</li> <li>• Assets – purchase, leasing, sales, rent, revenue, income, maintenance.</li> <li>• HR Strategy – training, development, health, etc.</li> </ul>		

### Appendix 3 – Risk Assessment Criteria





<b>LIKELIHOOD</b>	Event is almost certain to occur in most circumstances	>70%	Almost Certain	A					
	Event likely to occur in most circumstances	30-70%	Likely	B					
	Event will possibly occur at some time	10-30%	Possible / Moderate	C					
	Event unlikely and may occur at some time	1-10%	Unlikely	D					
	Event rare and may occur only in exceptional circumstances	<1%	Rare	E					
					5	4	3	2	1
					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	Significant impact on 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	Serious adverse local or minor adverse regional or national media public attention	Serious negative regional or national criticism	Prolonged regional & national condemnation
Financial Cost (£)					< £50k	£50k - £250k	£250k - £750k	£750k - £3m	>£3m
					<b>IMPACT</b>				

**Corporate Risk Severity Key**

	Minor	Risk easily managed locally – no need to involve management
	Moderate	Risk containable at service level – senior management and SLT may need to be kept informed
	Major	Intervention by SLT and / or Executive Committee involvement
	Critical	Significant SLT and Executive Committee intervention

## Appendix 4 – Project Risk Assessment Criteria

LIKELIHOOD	Event is almost certain to occur in most circumstances	>70%	Almost Certain	A					
	Event likely to occur in most circumstances	30-70%	Likely	B					
	Event will possibly occur at some time	10-30%	Possible	C					
	Event unlikely and may occur at some time	1-10%	Unlikely	D					
	Event rare and may occur only in exceptional circumstances	<1%	Rare	E					
						5	4	3	2
					Insignificant	Minor	Moderate	Major	Catastrophic
<b>Time / Objectives /Scope</b>					Insignificant increase to project time. Barely noticeable impact on project scope or objectives	<5% increase to project time. Minor impact on project scope or objectives	5% - 20% increase to project time . Major impact on project scope or objectives requiring SRO approval	20% - 50% increase to project time. Impact on project scope or objectives unacceptable to SRO	>50% increase to project time. Project fails to meet objectives or scope
<b>Reputation</b>					Trust recoverable with little effort or cost	Trust recoverable at modest cost with resource allocation within budgets	Trust recovery demands cost authorisation beyond existing budgets	Trust recoverable at considerable cost and management attention	Trust severely damaged and full recovery questionable and costly
<b>Financial Cost (£)</b>					Insignificant increase to project cost.	<5% increase to project cost.	5% - 20% increase to project cost.	20% - 50% increase to project cost.	>50% increase to project cost.
<b>IMPACT</b>									

Severity	Management intervention
 Minor	Report the new risk through the Highlight Report and Risk Register at the next meeting of the Project Board. Project Manager to monitor and manage the risk through the normal risk arrangements.
 Moderate	Email the new risk to the SRO for agreement of the mitigating actions. Report the through the Highlight Report and Risk Register at the next meeting of the Project Board. Project Manager to monitor and manage the risk through the normal risk arrangements.
 Major	Email the new risk to the SRO for agreement of the mitigating actions before emailing to the Project Board for agreement. Project Manager to monitor and manage the risk providing weekly updates to the SRO.
 Critical	Email the new risk to the SRO for agreement of the mitigating actions before emailing to the Project Board for agreement. SRO to alert the SLT of the risk at their next meeting. Project Manager to monitor and manage the risk providing weekly updates to the SRO.

## Appendix 5 – Risk Register Template

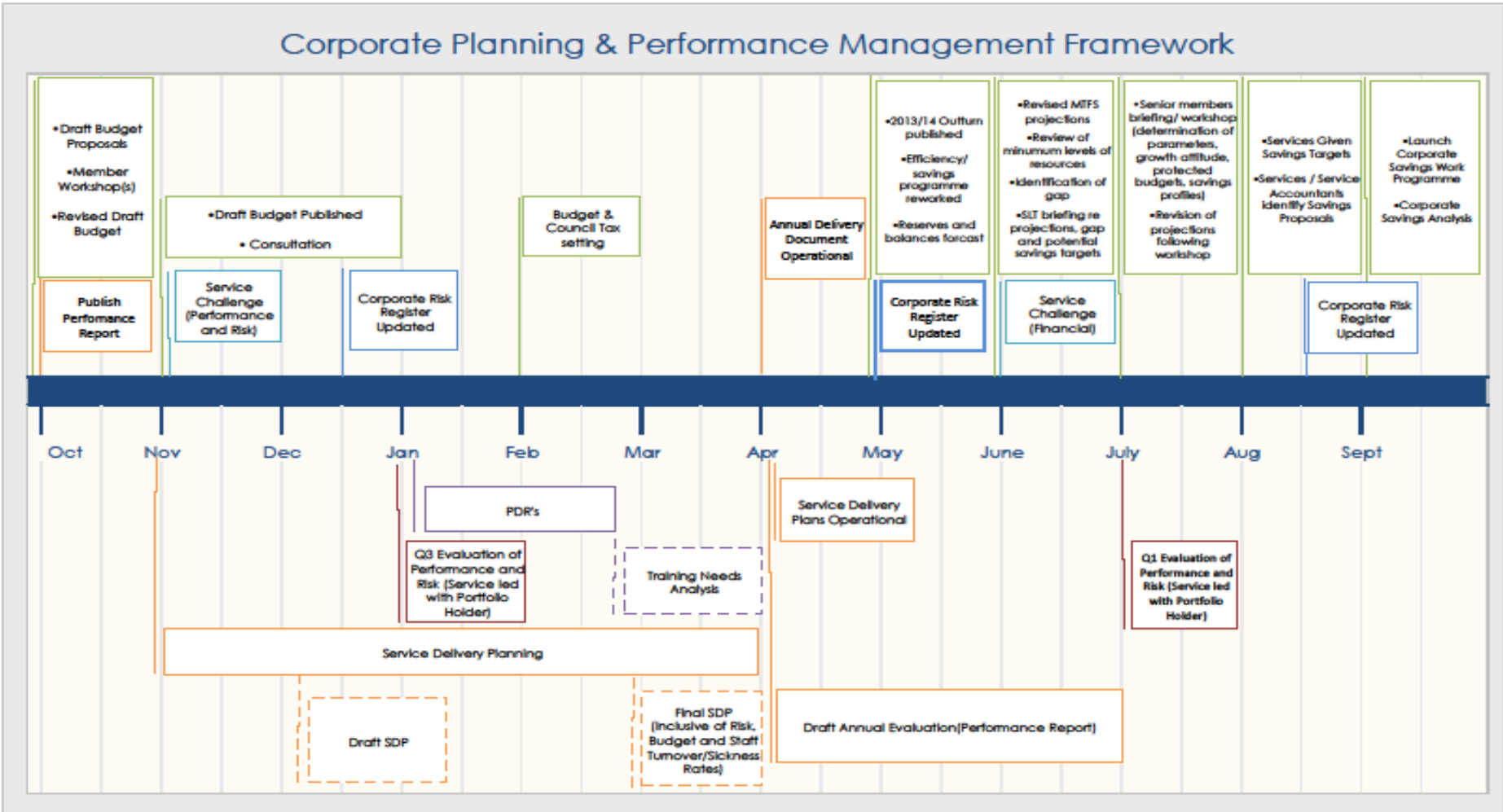
Please note the following is an outline only. A full risk register template is available as a separate Microsoft Excel document.

<Enter Service Name>

Updated: DD.MM.YY

Risk ID	Risk	Impact / Consequences	Risk Owner	Inherent Risk			Existing Controls	Residual Risk			Additional Action Required			Review Frequency
				Likelihood	Impact	Score		Likelihood	Impact	Score	Action	Responsible Officer	Target Date	

# Appendix 6 – Corporate Planning & Performance Management Framework



## Appendix 7 – Glossary of Terms

**Control** – an existing process, policy, practice or other action that acts to minimize negative risk or enhance positive opportunities. The word ‘control’ can also be applied to a process designed to provide reasonable assurance regarding the achievement of objectives.

**Event** – occurrence of a particular set of circumstances. An event can be certain or uncertain. An event can be a single occurrence or a series of occurrences.

**Impact** – outcome or impact of an event. There can be more than one impact from one event. Impacts can range from positive to negative. Impacts can be expressed qualitatively or quantitatively. Impacts are considered in relation to the achievement of objectives

**Issue** – refers to the consequences of a risk are already with us and management mitigation actions are underway or planned. In a project environment an issue is a point or matter in question or in dispute, or a point or matter that is not settled but is under discussion or over which there are opposing views or disagreements.

**Likelihood** – describes the extent to which an event is likely to occur. Likelihood can be expressed qualitatively or quantitatively. Probability or frequency may be used in describing a risk.

**Risk** – an event that, should it occur, would impact our ability to successfully achieve our business objectives. Risk is a measure used to describe the uncertainty surrounding an event and its potential impact.

**Residual risk** - risk remaining after consideration of existing controls and their effectiveness.

**Inherent risk** - risk before consideration of existing controls and their effectiveness.

**Target risk** – future risk level expected after planned risk mitigation actions are completed.

**Project** - a temporary structure that is created for the purpose of delivering one or more business products according to an agreed business case in an agreed time frame and with a set budget.

**Risk assessment** - the overall process of risk identification, analysis, action planning and reviewing.

**Risk Register** – the document where we record our risks.