

**RIBBLE VALLEY BOROUGH COUNCIL**  
**REPORT TO ACCOUNTS AND AUDIT COMMITTEE**

DECISION

Agenda Item No 10

meeting date: 26 JULY 2017  
title: RISK MANAGEMENT POLICY REVIEW  
submitted by: DIRECTOR OF RESOURCES  
principal author: SALMA FAROOQ

1. PURPOSE

- 1.1. To ask Members to consider the approval of the updated and revised Risk Management Policy.
- 1.2. Relevance to the Council's ambitions and priorities:
  - Community Objectives – none identified.
  - Corporate Priorities – to be a well-managed Council.
  - Other Considerations – none identified.

2. BACKGROUND

- 2.1. A comprehensive review of the policy has been undertaken and committee are now asked to consider the revised policy attached at Appendix A for approval.

3. INFORMATION

- 3.1. There have been slight changes to the policy and this was to reflect updated regulations and procedures.
- 3.2. One of these changes includes the Risk Management Working Group no longer being in place. The original purpose of the Risk Management Working Group had been to implement the new risk management policy in 2010 and this is no longer applicable.

4. FURTHER POLICY REVIEWS

- 4.1 A number of further policies are currently being reviewed and will be brought to your next meeting in October for consideration and approval. These are:
  - Whistleblowing Policy
  - Anti-Fraud and Corruption Policy
  - Procurement Strategy

5. RECOMMEND THAT COMMITTEE

- 5.1 Note the amendments to the Risk Management Policy and approve the reviewed Risk Management policy.

SENIOR AUDITOR

DIRECTOR OF RESOURCES

AA14-17/SF/AC  
12 July 2017

BACKGROUND PAPERS

None

For further information please ask for Salma Farooq.

---

# Risk Management Policy

---

July 2017

---



Ribble Valley  
Borough Council

---

[www.ribblevalley.gov.uk](http://www.ribblevalley.gov.uk)



# Contents

Section	Page
Risk Management Policy Statement	4
What is Risk Management	4
The Risk Management Cycle	5
The Benefits of Risk Management	6
The Cost of Risk	7
Why we Need to Manage Risk	7
Risk Management Aims and Objectives	8
Roles and Responsibilities	8
Inter-Relationships to Support the Risk Management Strategy	11
Risk Management Process	13
Categories of Risk	16
Promoting Risk Awareness	17
The Turnbull Report	18
Annex 1 – Guidance on Assessing the Likelihood and Impact Levels of a Risk	20

## Key Officer Contacts

Name	Post	Email Address
Lawson Oddie	Head of Financial Services	lawson.oddie@ribblevalley.gov.uk
Salma Farooq	Senior Auditor	salma.farooq@ribblevalley.gov.uk

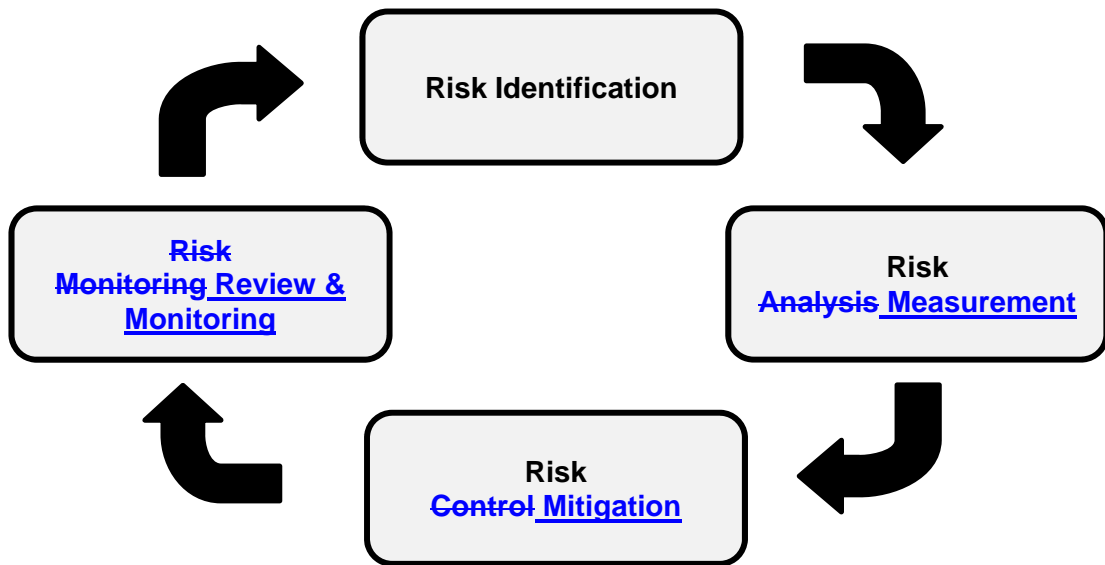
## 1. Risk Management Policy Statement

- 1.1. The Council recognises that it authority has a moral and statutory duty to take all reasonable actions to safeguard its employees, assets and the public and ensure that it is not financially or operationally disrupted. It will meet this duty by ensuring that risk management plays an integral part in the governance of the authority at a strategic and operational level.
- 1.2. The purpose of this policy is to clearly outline the Council's commitment to risk management, describe the objectives of risk management and provide a framework for embedding risk management across the organisation, with defined roles and responsibilities and a structured process.
- 1.3. ~~The Risk Management Working Group will support the authority in fulfilling this duty. However, r~~Risk management is an active process that requires the co-operation of all staff. Thus, the management of risk is not the responsibility of any one person or group, but the responsibility of every individual in the authority.
- 1.4. The Council is aware that risks can never be fully eliminated and has a policy in place that provides a structured, systematic and focused approach to managing risk. However, risk management is not about being risk averse, it is about being risk aware.
- 1.5. Insurable losses are the responsibility of the authority, not that of an insurance company. Management has the responsibility to plan and systematically approach the identification, analysis and control of risk.

## 2. What Is Risk Management?

- 2.1. Risk Management is the process of identifying risks, evaluating their likelihood and potential impact and determining the most effective methods of controlling them or responding to them. ~~identification, analysis and economic control of those risks that can threaten the assets of an organisation or the ability of the organisation to provide a service.~~
- 2.2. Risk Management should not be seen as a "bolt on"; it should be integral to policy planning and operational management within the authority. Applying the risk management cycle will help elected members and managers make informed decisions about the appropriateness of adopting policy or service delivery options.
- 2.3. The risk management cycle will generate information that will help ensure that risks can be avoided or minimised in the future. It will also enlighten judgements on the type and degree of insurance cover and the balance to be reached between self-insurance and external protection.

### 3. The Risk Management Cycle



#### Risk Identification

- 3.1. Identifying and understanding the risks that the authority faces is essential for informed decisions to be made about policies or service delivery methods. The risk associated with these decisions can then be effectively managed.

#### Risk Analysis Measurement

- 3.2. Once the risks have been identified they need to be systematically analysed using proven analysis techniques and all available data on the potential frequency and consequences of events. If a risk is seen to be unacceptable steps need to be taken to control or respond to it.

#### Risk Control Mitigation

- 3.3. Risk Control mitigation is the process of taking action to reduce the chance of a risk occurring and /or the impact of the risk should it occur. These factors should be reduced to the lowest point where the action taken is still economical. Risk control often requires projects to be implemented or operating procedures to be revised.

#### Risk Monitoring Review & Monitoring

- 3.4. To complete the risk management process, all risk control projects and revisions in operating procedure need to be monitored and reviewed. It is also important to assess whether the nature of the risk has altered with time.

- 3.5. New/ emerging risks should be considered on the risk register and those that are no longer considered a risk should be removed.

- 3.6. Failure to pay proper attention to the likelihood and consequences of risk could cause great damage to the authority. Some examples of damage include service disruption, threat to public health, financial costs, compensation claims and bad publicity. The management of risk is consequently a key part of the authority's approaches to the delivering of the sound governance element of Best Value

### 4. The Benefits of Risk Management

- 4.1. The benefits of managing risk effectively include:

#### Improved Strategic Management

- Better informed selection of strategic objectives and related targets as a result of the risk identification, analysis, control and monitoring process.
- Enhanced ability to deliver against more realistic and attainable objectives and targets.

## Improved Operational Management

- ~~Decline in the number of~~Reductions in interruptions to service delivery.
- Reduction in managerial time devoted to managing the results of a risk event having taken place.
- Improved managerial control as a result of risk identification, analysis, control and monitoring.
- A more systematic method to addressing legislative, regulatory or competitive demands.
- Improved health and safety and the superior condition of property and equipment.

## Improved Financial Management

- ~~Decrease in the financial costs linked with losses due to service interruption, litigation, bad investment decisions, etc.~~
- Better-informed financial decision-making~~on investment, insurance, option appraisal, etc.~~
- Improved financial control as a result of risk identification, analysis, control and monitoring.
- Reduction in insurance premiums and direct costs met through self-insurance.

## Improved Public Service

- Minimal service disruption to public and a positive external image as a result of all of the above.

## 5. The Cost of Risk

- 5.1. The cost of risk is made up of two components, the evident cost of risk and the hidden cost of risk. The evident cost of risk are things such as insurance premiums, uninsured losses met from the revenue budget, the cost of risk control measures and direct administration costs. ~~According to the Association of Local Authority Risk Managers (ALARM) the average local authority has an evident cost of risk in excess of 0.65% of gross revenue.~~
- 5.2. The hidden cost of risk can be much harder to identify and evaluate. The hidden cost can include things such as a fall in staff morale, the cost of management time spent dealing with the risk events, damage to the reputation of the authority, indirect administration costs and the cost of employees being off work following an accident. It is widely thought that the hidden cost of risk can be many times that of the evident cost. ~~To calculate the hidden cost of risk ALARM use a multiplier of eight times the evident cost, which they consider to be a conservative estimate. For some authorities the multiplier can be as high as thirty times. This means that the total cost of risk for the authority is likely to be at least 5.2% of gross revenue (£1.1m) and could even be much higher.~~
- 5.3. Association of Local Authority Risk Managers (ALARM) says that experience in the private sector proves that the cost of risk can be reduced in real terms by the implementation of risk management. With the cost of risk being so high any action that can reduce this cost will be of benefit to the whole authority.

## 6. Why We Need To Manage Risk

- 6.1. In the current economic climate with severe pressures on funding for services and the need for greater efficiencies whilst improving services means that sound corporate governance and good decision making are paramount.
- 6.2. The Council has a statutory responsibility to have in place arrangements for managing risks. As stated in the Account and Audit Regulations 20032012 (Part 2, Section 4):

*The relevant body shall be is responsible for ensuring that the financial management of the body is adequate and effective and that the body has a sound system of internal control which facilitates the effective exercise of the that body's function and which includes arrangements for the management of risk.*

- 6.3. ~~Risk management is recognised as an important element of good corporate governance.~~ Effective risk management arrangements are a key element within the Council's governance framework. The CIPFA/SOLACE Framework on Corporate Governance requires councils to establish and maintain a systematic strategic and methodological process for managing risk. They must also report publicly on the effectiveness of these arrangements.



6.4. Risk Management is beneficial to Ribble Valley Borough Council as it:

- Helps us to be more flexible and responsive to new internal and external demands.
- Helps the Council make informed decisions.
- Provides assurance to Members and management.
- Reduces incidents and other control failures.
- Helps in the achievement of the Councils' objectives.

## 7. Risk Management Aims and Objectives

7.1. By implementing the risk management policy the authority aims to:

- [Preserve and protect the Council's assets, reputation and staff.](#)
- Provide continuous high quality services to the residents of Ribble Valley.
- [Use appropriate identification and analysis techniques to identify risks to the authority and determine the long and short term impact. Anticipate and respond to changing social, economic, environmental and legislative requirements.](#)
- Prioritise and implement economic control measures to reduce or remove risks.
- Protect and promote the reputation of the authority in the community.
- Through the use of education, training and communication, develop and maintain a structured risk management culture, where risk is considered in the decision making process and the everyday working situations of all personnel.
- Maintain a system for recording and providing accurate, relevant and timely risk management information.
- Reduce the long-term cost of risk to the authority.

## 8. Roles and Responsibilities

8.1. Risk Management roles and responsibilities of key positions are outlined below:

### **Accounts and Audit Committee**

#### **Role**

- Overall responsibility for Risk Management
- ~~A member of the Committee is the Council's 'Member Champion'.~~
- Ensure that a comprehensive approach to risk management is developed and implemented by management.

#### **Responsibilities**

- To attain a knowledge of risk management and its benefits.
- [To oversee the effective management of risk by the senior management of the authority.](#)
- [Receive regular reports on the management of the Council's red risks.](#)

## **Corporate Management Team**

### ***Role***

- To ensure that the authority manages risk systematically, economically and effectively through the development of an all-encompassing corporate strategy.

### ***Responsibilities***

- To acquire a knowledge of risk management and its benefits.
- To help develop the risk management strategy and communicate it to the elected members.
- To promote and oversee the implementation of the strategy across the authority.
- To assist in monitoring and reviewing the risk management strategy through monthly reports taken to CMT, including an annual review of its effectiveness and a written report of this to stakeholders.
- To agree any inputs and resources necessary to support the implementation of the strategy corporately.

## **~~Risk Management Working Group~~**

### **~~*Role*~~**

- ~~• To support the authority in the development, implementation and review of the risk management strategy.~~
- ~~• To share experiences on risk, risk management and strategy implementation across the authority.~~

### **~~*Responsibilities*~~**

- ~~• To develop the risk management strategy in liaison with the Corporate Management Team.~~
- ~~• To promote, support and oversee its implementation across the authority.~~
- ~~• To identify any dedicated inputs and resources required to support the implementation of the strategy.~~
- ~~• To identify and communicate risk management issues to the different service areas.~~
- ~~• To assist service areas in undertaking risk management activity through training and/or direct support.~~
- ~~• To monitor, review and report the effectiveness of the risk management strategy.~~
- ~~• To share good practice on all elements of risk management.~~

## **Heads of Service**

**Role**

- To manage risk in each particular service area.

**Responsibilities**

- To contribute to the development of the risk management strategy from a function specific perspective.
- To disseminate the detail of the strategy and allocate responsibilities for implementation of the strategy in their service area.
- To recommend the necessary training on risk management for the employees in the section.
- To share relevant information with other service sections.
- To identify any risk management issues in their service area.
- ~~To provide feedback to the Risk Management Working Group on their experience of implementing the strategy and their perceptions of the effectiveness of the strategy.~~
- To ensure that the strategy is implemented across the function.

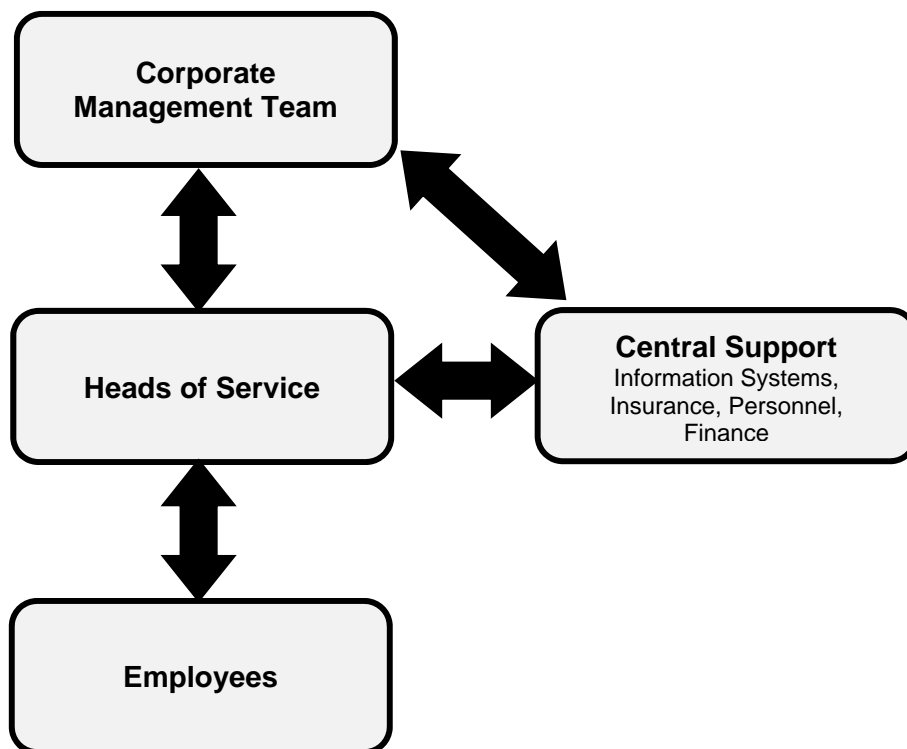
**Employees****Role**

- The management of risk in their own work.

**Responsibilities**

- To liaise with their manager to assess areas of risk in their job.
- To identify and alert their manager of new or changing risks in their job.
- To effectively use skills and knowledge that they have gained through training.
- To carry out their job within the risk management guidelines set down by their manager.

9. Inter-Relationships to Support the Risk Management Strategy

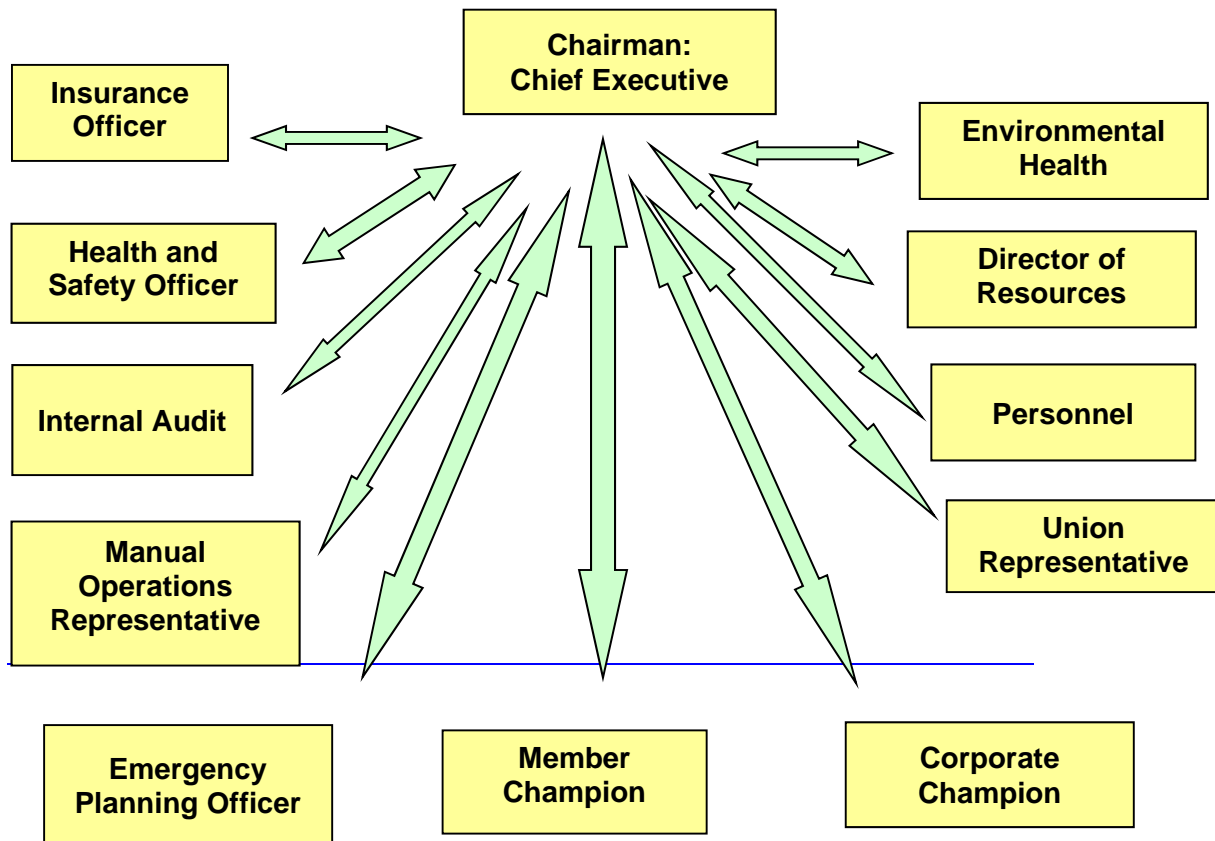


9.1. The arrows represent the flow of guidance, information and feedback within the structure. [Communications regarding the risk management issues should be open as outlined in the Turnbull Report.](#)

## Risk Management Working Group

The Chief Executive chairs the Risk Management Working Group. He is committed to the concept of risk management. The body of the group is made up of representatives from different service areas. These staff have a sound knowledge of risk management and are willing to dedicate time and effort to the implementation of the strategy.

### Risk Management Working Group Structure



The Risk Management Working Group meet on a quarterly basis and have a set agenda of items to be covered. From this it can be determined where there are issues concerning risk management and where action needs to be taken.

Regular reports on risk management are sent to Accounts and Audit Committee.

## **10. Risk Management Process**

10.1. The Council's risk management process is underpinned by a series of consistent processes and documentation that:

- Identify and manage risks in a consistent, holistic way across the Council;
- Focus on risks that, because of their likelihood and impact, make them management priorities.

10.2. The Councils' risk management process is also supported by the use of GRACE risk management software. The software enables Managers to have access to their risks and to prioritise them accordingly.

10.3. The GRACE risk management software allows the Council to:

- Record identified risks and manage them in a consistent way.
- Map risks to corporate and operational objectives, PI's and risk types.
- Generate risk registers.
- Identify key risks.
- Record mitigating actions.
- Monitor and review risks, including tracking changes to risks.
- Produce both generic and customised management reports.

### **Step 1 – Define Objectives**

10.4. Ribble Valley Borough Council's objective is to be a 'well managed council providing efficient services based on identified customer needs'. This aim is underpinned by the Council's objectives.

10.5. As well as corporate objectives there are also service objectives, which have been drawn up by Heads of Service. Each service objective impacts upon corporate objectives and in turn the Council's overall objectives.

### **Step 2 – Identify Risks**

10.6. Risk identification attempts to identify the Council's exposure to uncertainty. Generic risk profiles have been supplied by Grace Governance Solutions Ltd, however it is important to remember that not all risks as listed in the generic profiles may be relevant and therefore risk owners are responsible for identifying the applicable risks as listed in the generic profiles and any additional risks not listed that the service/department faces.

10.7. Having identified the risks, these are recorded on a Risk Register. All risk registers are created and maintained on the GRACE risk management system. Risks are identified on a strategic, operational, directorate, partnership and project level.

### Step 3 –Assess Risks

- 10.8. Risks are assessed by looking at the likelihood of the risk occurring and the impact that risk would have if it were to occur. Controls are probably in place to minimise identified risks, however, in the first instance risks are assessed as though there were no controls in place i.e. the worst case scenario. This is known as the ‘**gross**’ risk level. The gross risk level is recorded in the risk register.
- 10.9. In most scenarios however there will be controls in place to minimise the likelihood or impact of the identified risk occurring. Risks are therefore assessed based on the likelihood and impact of the risk occurring considering that there are mitigating actions in place. This is known as the ‘**net**’ risk level. The net risk level is recorded in the risk register.
- 10.10. Each risk is allocated a risk owner whose name is recorded on the risk register. Guidance on how the likelihood and impact levels of a risk should be assessed can be found in Annex A.

### Step 4 – Prioritise Risks

- 10.11. Some risks command a higher priority due to their likelihood and impact. Both the gross and net likelihood and impact levels of each risk are plotted and prioritised using a 3 x 3 matrix as can be seen below:

<b>IMPACT</b>	<b>HIGH</b>	<b>Amber 6</b>	<b>Red 8</b>	<b>Red 9</b>
	<b>MEDIUM</b>	<b>Green 3</b>	<b>Amber 5</b>	<b>Red 7</b>
	<b>LOW</b>	<b>Green 1</b>	<b>Green 2</b>	<b>Amber 4</b>
		<b>LOW</b>	<b>MEDIUM</b>	<b>HIGH</b>
<b>LIKELIHOOD</b>				

- 10.12. A ‘traffic light’ system is used to show high (red), medium (amber) and low (green) risks. This results in the prioritisation of both gross and net risks, which are recorded in the risk register.

### Step 5 – Respond to Risks

- 10.13. As most risks cannot be eliminated altogether, judgments have to be made as to what level of risks are acceptable. There are four categories of response – transfer, treat, terminate and tolerate. Details of each response can be found in the following table:

Response	Description
<b>Transfer</b>	<p>Risks are transferred to an insurer, e.g., legal liability, however it must be remembered that this is not possible for all risks.</p> <p>Some service delivery risks can also be transferred to a partner or contractor by way of a formal contract or written agreement.</p> <p>Some risks however cannot be transferred, for example, reputational risks.</p>
<b>Treat</b>	<p>Risks need additional treatments (controls) to reduce the likelihood and impact levels.</p> <p>This response is most likely where the risk has been identified as a high risk due to the likelihood and impact levels.</p>
<b>Terminate</b>	<p>A risk is identified as being so serious that there is no option other than to terminate the activity generating the risk.</p>
<b>Tolerate</b>	<p>The controls in place reduce the likelihood and impact levels to a tolerable level. It is therefore decided to <i>tolerate</i> the risk.</p>

10.14. Generally any 'net' red risks (i.e. after mitigating action has been considered) are viewed as unacceptable and must be treated. It may be necessary to carry out a cost benefit analysis to ensure that the cost of introducing further mitigating action(s) does not outweigh the cost of tolerating the risk.

10.15. Amber risks are acceptable; however, the risk should be reduced as low as is reasonably practicable and contingency plans must be developed. Green risks are broadly acceptable.

10.16. The acceptance of a risk represents an informed decision to accept the impact and likelihood of that risk. A risk owner must be allocated to each identified risk. This ensures the 'ownership' of the risk is identified and that the appropriate resources are allocated. Risk owners are responsible for:

- Ensuring that appropriate resources and importance are allocated to the process;
- Confirming the existence and effectiveness of the mitigating actions and ensuring that any proposed mitigating actions are implemented;
- Providing assurance that the risks for which they are Risk Owner are being effectively managed.

### Step 6 – Monitor Risks

10.17. Risks are monitored at the following frequency:

<b>Red</b>	High risk, monthly
<b>Amber</b>	Medium risk, quarterly



Green

Low risk, 6 monthly

### Step 7 – Review and Report

- 10.18. Reports are sent to Accounts and Audit Committee at each meeting informing them on the progress to date with regards risk management. A copy of the most recent red risk register is also included in these reports.
- 10.19. Risk Owners not carrying out risk reviews in accordance with the frequency schedule as listed above are also reported to the Councils' Corporate Management Team on a monthly basis.
- ~~The Risk Management Working Group meets on a fairly ad-hoc basis, but usually quarterly.~~

### Step 8 – Communicate and Consult

- 10.20. Copies of this policy are available on both the Intranet and Internet. [Step by step notes for updating risks on GRACE are held on the Intranet. One to one training is provided to new responsible risk owners.](#)
- ~~• Risk Management Training has been provided as follows:~~
  - ~~• November 2005 – Risk owner training on the GRACE system~~
  - ~~• March 2006 – Staff training~~
  - ~~• May 2006 – Risk owner training~~
  - ~~• April 2008 – Risk owner and member training~~

## 11. Categories of Risk

- 11.1. Risks can be strategic or operational.

**Strategic:** risks that need to be taken into account in judgements about the medium to long-term goals and objectives of the authority.

- Political – Those connected with the failure to deliver either local or central government policy.
- Economic – Those affecting the authority's ability to meet its financial commitments. These include internal budgetary pressures, the failure to purchase sufficient insurance cover or the effects of proposed investment decisions.
- Social – Those relating to the consequences of changes in demographic, residential or socio-economic trends on the authority's ability to meet its objectives.
- Technological – Those associated with the authority's ability to cope with the scale and pace of technological change, and its ability to use technology to meet changing demands.
- Legislative – Those associated with present or future national and European law.
- Environmental – Those relating to the environmental consequences of progressing the authority's strategic objectives (e.g. in terms of pollution and energy efficiency).

- Competitive – Those concerning the competitiveness of the service in terms of cost or quality and/or its ability to deliver [Best Value best value for money](#).
- Customer/Citizen – Those connected with the failure to meet the present and shifting needs and expectations of the customers and citizens.

**Operational:** risks encountered in the everyday work of managers and staff.

- Professional – Those involved with the specific nature of each profession.
- Financial – Those linked to financial planning and control and sufficiency of insurance cover.
- Legal – Those connected to possible violations of legislation.
- Physical – Those associated with fire, accident prevention and health and safety.
- Contractual – those related to the failure of contractors to deliver services or products to the agreed cost or specification.
- Technological – Those linked with the reliance on operational equipment.
- Environmental – Those relating to pollution and energy efficiency of ongoing service operations.

## **12. Promoting Risk Awareness**

- 12.1. Increasing risk awareness is a very important part of implementing the risk management strategy as it helps to develop a risk management culture.
- 12.2. Officers from across the authority have been involved in risk management training sessions and an overview with regards risk management has been published on the Intranet. [One to one training is provided to new responsible risk owners.](#)

### 13. The Turnbull Report

#### What is the Turnbull Report?

- 13.1. The Turnbull Report is guidance on the implementation of the internal control requirements of the Combined Code on Corporate Governance. It was written by The Institute of Chartered Accountants in England and Wales and has the full support of the London Stock Exchange. It provides guidance to assist companies to implement principle D2 of the Combined Code of Corporate Governance, i.e.

*The board should maintain a sound system of internal control to safeguard shareholders' investment and the company's assets.*

- 13.2. A system of internal control is made up of the policies, processes, tasks, behaviours and other aspects of an organisation that:
- Facilitate its effective and efficient operation by enabling it to respond to risks to achieving the organisation's objectives. These include significant business, operational, financial and compliance risks. The safeguarding of assets and identification and management of liabilities are also included in this.
  - Help ensure the quality of internal and external reporting. Records and processes that produce a flow of information should be maintained so that information is timely, relevant and reliable, whether from within or out with the organisation.
  - Assist in ensuring compliance with laws, regulations and internal policies with respect to the conduct of business.

#### Why Does It Affect Ribble Valley Borough Council?

- 13.3. The Turnbull Report only applies to UK listed companies; however it is beneficial for other organisations to follow the guidelines. It is seen as "best practice" and "the sort of thing that companies should be doing anyway" according to Roger Davis, deputy chairman of the Turnbull Committee.
- 13.4. Former Chief Executive of ALARM (1999-2001), Liz Taylor, made it clear that she believes that life in the public sector is about to change as a result of increasing concentration on good corporate governance.

*Guidelines drawn up for the private sector are beginning to influence management thinking in the public sector," she said. "Senior managers must keep abreast of the changes in corporate governance guidelines and legislation within the private sector.*

*Change is definitely coming, and managers within the public sector need to get a grasp of it so that they are in control when it arrives. They should read the Turnbull Committee's report and review their strategies in light of its recommendations.*

- 13.5. Although the Turnbull Report is not aimed at the public sector, it is a complete codification of good practice and so should not be ignored.

#### What Are the Implications of the Turnbull Report on the Authority?

- 13.6. The Turnbull Report requires a sound system of internal control, safeguarding the shareholders' investment and the company's' assets, to be maintained by the board. On deciding what is a sound system of internal control, the following will need to be

considered:

- The nature and extent of risks facing the authority.
- The extent and categories of risk which it regards acceptable for the authority to bear.
- The likelihood of those risks concerned materialising.
- The authority's ability to reduce the incidence and impact on the organisation of the risks that do materialise.
- The cost of operating particular controls relative to the benefit thereby obtained in managing the risk.

- 13.7. Continuous effective monitoring is an essential part of a sound system of internal control. The Turnbull report requires the Board, or in the case of the Council the Corporate Management Team, to regularly review reports on the effectiveness of the system of internal control. The reports that they review should provide a balanced assessment of the significant risks and the effectiveness of the systems of internal control. Any major failings must be discussed in the reports, including the possible impact and actions being taken to rectify them.
- 13.8. An annual assessment of the effectiveness of the Councils' system of internal control is carried out and is reported to stakeholders. The review covers risk management and all controls, including financial, operational and compliance controls.
- 13.9. The annual reports and accounts also contain a narrative account of how the Council has applied the above principles, providing explanations, which enable the stakeholders to evaluate how the principles have been applied. Or if there has been a period of non-compliance, detail the nature of and reasons for the non-compliance.
- 13.10. To follow the guidelines of the Turnbull Report the management of risk should not be treated as a separate exercise; it should be embedded within the organisation, forming part of its culture. It should be at the top level of governance within the organisation. The authority should identify, evaluate and manage significant risks and also be able to respond to changing risk. However the authority should not eliminate all risk as some risks can produce positive results. There should be openness of communication on matters relating to risk management.
- 13.11. The report also requires that all employees have some responsibility for managing risk as part of their accountability for achieving objectives. They should have the knowledge, skills, information and authority to operate and monitor a system of internal control.
- 13.12. This risk management policy document has been drawn up to be in line with the guidelines of the Turnbull Report. In following this document, the key recommendations of the report will be fulfilled by the authority.

## GUIDANCE ON ASSESSING THE LIKELIHOOD AND IMPACT LEVELS OF A RISK

## Likelihood

Description	Example Detail
High (Red)	<ul style="list-style-type: none"> <li>Has <b>happened</b> in the past year; or is <b>expected</b> to happen in the next year</li> <li>More than <b>50% probability</b></li> </ul>
Medium (Amber)	<ul style="list-style-type: none"> <li>Has <b>happened</b> in the past 2-5 years; or is <b>expected</b> to happen in the next <b>2-5 years</b></li> <li>Between <b>25% to 50% probability</b></li> </ul>
Low (Green)	<ul style="list-style-type: none"> <li>Has <b>not happened</b> in the past <b>5 years or more</b>; or is <b>not expected</b> to happen in the next <b>5 years or more</b></li> <li>Between <b>1% to 25% probability</b></li> </ul>

## Impact

Description	Example Detail
High Red	<ul style="list-style-type: none"> <li>Death or life threatening</li> <li>Serious service failure impacts on vulnerable groups</li> <li>Negative national publicity or widespread adverse local publicity</li> <li>Serious impact felt across more than one Directorate</li> <li>Legal action almost certain and difficult to defend</li> <li>Financial impact not manageable within existing funds and requiring Member approval for virement or additional funds in excess of £100,000</li> <li>Non-compliance with law resulting in imprisonment</li> </ul>

Description	Example Detail
<p style="text-align: center;"><b>Medium Amber</b></p>	<ul style="list-style-type: none"> <li>• Extensive, permanent/long term injury or long term sick</li> <li>• Service failure impacts on property or non-vulnerable groups</li> <li>• Negative local publicity but not widespread</li> <li>• Expected impact, but manageable within Directorate contingency plans</li> <li>• Legal action expected</li> <li>• Financial impact not manageable within existing Directorate budget and requiring the Director of Resources approval for virement or additional funds i.e. between £50,000 and £100,000</li> <li>• Non-compliance with law resulting in fines</li> </ul>
<p style="text-align: center;"><b>Low Green</b></p>	<ul style="list-style-type: none"> <li>• Short term sickness absence, first aid or medical treatment required</li> <li>• Some risk to normal service but manageable within contingency arrangements</li> <li>• Little if any scope for impact on vulnerable groups</li> <li>• Negative customer complaints</li> <li>• Possible impact, but manageable locally by Head of Service</li> <li>• Legal action possible but unlikely and defensible</li> <li>• Possible financial impact manageable within Directorate budget i.e. less than £50,000</li> <li>• Non-compliance with regulations/standards or local procedures resulting in disciplinary action</li> </ul>



## Producing a District Emergency Planning Risk Register

### 1. Introduction

In the past when Local Authority External Inspectors requested sight of an Authority's Emergency Planning Risk Register they would accept a copy of the Community Risk Register prepared by the Resilience Forum of which the Authority was a member. This is now changing – instead the Inspectors are expecting the preparation and maintenance of an Authority **specific** Emergency Planning Risk Register.

### 2. History

For many years Ribble Valley Borough Council has maintained Risk Registers for each of their functions, services and operations using risk management software supplied by Grace Governance Solutions Ltd (Gracegs Ltd) who also supply Interactive Generic Risk and Control Profiles Library.

The Interactive Generic Profiles Library is a tool designed to be used as a reference source on its own, tailored to an authority, and/or to assist in the compilation of a risk register, risk profiles, audit programmes, populate risk management and corporate governance reporting software.

They are supplied in an Interactive Format to enable Emergency Planning Officers, Risk Managers etc. to select a risk, then view suggested controls and then the associated compliance tests. The text can be copied and pasted.

In 2008 Ribble Valley Borough Council and Gracegs Ltd worked together to formulate a new module to be added to the Generic Profiles Library – Emergency Planning – consisting of 16 profiles.

Profiles were formulated for each category prescribed by the UK risk assessment framework (provided by the Office of the Deputy Prime Minister (ODPM)). In addition an Emergency Planning and Management profile was formulated.

The profiles were formulated using a variety of sources including:

1. Lancashire Resilience Forum Community Risk Register
2. Community Risks Registers in the public domain
3. Output from Emergency Planning Risk and Control identification workshops
4. Officers knowledge and experience
5. Articles and publications

They reflect current guidelines, requirements and best practice.



### 3. Producing a District Emergency Planning Risk Register



~~Using the Grace Risk Management system officers at Ribble Valley Borough Council tailored each of the generic profiles to their Authority's environment, mapped the controls and set the risk levels.~~

~~Eighteen Emergency Planning Risk Registers were produced — there are 3 specific Flooding Risk Registers. These registers are regularly reviewed and updated by designated Emergency Planning officers — **Appendix A.**~~

~~Using the reporting facility the officers were then able to compile a Ribble Valley Borough Council Emergency Planning Risk Register — **Appendix B.**~~

#### **4. Availability/Access**

~~The Generic Risk and Control Emergency Planning Module has as a platform been called 'EMA' Emergency Management Assessment, in acknowledgement of the involvement of RVBC in this development 'EMA' will be provided on a continuing no cost basis. This arrangement will also be extended to those Authorities who are involved in the evaluation process for a limited period.~~

~~Authority's can compile their own specific District Emergency Planning Risk Register on a spreadsheet or populate risk management software they may have already installed/developed.~~

~~Authority's who wish to continue to maintain their Emergency Planning risk registers on the **Ema** (Emergency Management Assessment) software system can procure the final commercial product.~~

~~Ema is a version of the Grace software designed specifically for formulating and maintaining Emergency planning risk registers.~~

~~Ema will be accessible on the internet enabling users to access their data from any location from where they can make an internet connection.~~

~~Chris Shuttleworth 09092010~~