

Appendix 1



RISK MANAGEMENT STRATEGY

March 2007

Appendix 1

CONTENTS

1. Introduction
2. Definitions
3. Why have a Risk Management Strategy?
4. Risk Management Policy Statement
5. Roles and responsibilities
6. The Risk Management process
7. Performance Management
8. Relationships with existing processes
9. Reporting
10. Review

Appendix 1

Example “Risk Register and Management Action Plan”

Appendix 1

1. Introduction

- 1.2 This strategy provides an overview of the operating framework, arrangements and responsibilities for risk management within the Council. The strategy will be of relevance to Executive Directors as recipients of the service, elected Members with responsibility for overseeing the Council's risk management arrangements and members of the officer body charged with co-ordinating and facilitating development of the Council's risk management arrangements.
- 1.3 This strategy, together with the Risk Management Policy, will be reviewed annually under the direction of the Chief Internal Auditor and any significant amendments will be presented to the Audit Committee, as the member body responsible for overseeing the Council's risk management arrangements, for approval.
- 1.4 The risk management function is provided via the Internal Audit, Risk and Assurance Service within the Directorate of Resources. The service is lead by the Chief Internal Auditor with the support of the Risk and Controls Assurance Manager.

2. Definitions

- 2.0 Every organisation exists for a purpose – to achieve something – and every organisation can define its purpose in terms of objectives. The achievement or otherwise of those objectives depends upon:-
- the organisation doing certain things and not doing others;
 - the occurrence of (internally and externally caused) events that could affect the organisation; and
 - the circumstances in which the organisation finds itself.
- These events, circumstances, actions and inactions may or may not exist or occur and will, if they exist or occur, have an impact on the achievement of the organisation's objectives.
- 2.1 **Risk** can be defined as “the combination of the probability of an event and its consequences”.
- 2.2 **Risk Management** can be defined as the “the culture, processes and structures that are directed towards effective management of potential opportunities and threats to the organisation achieving its objectives”.
- 2.3 In other words, risk is one of life's certainties and how successfully the Council, a directorate or division deals with it can have a major impact on the achievement of its key business objectives.

Appendix 1

- 2.4 Risk Management is not simply a compliance issue. It should be a continuous and developing process that methodically addresses all significant business risks at both strategic and operational levels with a view to meeting objectives and supporting continuous improvement.

3. The need for a Risk Management Strategy

- 3.1 The Risk Management Strategy sets out the roles and responsibilities for managing risk which will, in turn, help to improve co-ordination of risk management activity throughout the Council, reduce duplication in terms of managing overlapping risks and provide a framework for managing risk.
- 3.2 The development of a Risk Management Strategy and Policy is in line with good practice contained within “The Risk Management Standard Document” published by the Institute of Risk Management (“IRM”), the Association of Insurance and Risk Managers (“AIRMIC”) and the Association of Local Authority Risk Managers (“ALARM”).
- 3.3 The Comprehensive Performance Assessment (“CPA”) Use of Resources includes specific and detailed reference to risk management in the “Internal Control” key line of enquiry. There is an expectation that the Risk Management Policy and Strategy is in place and has been formally approved by Members.
- 3.4 Risk management is an integral part of good governance particularly in relation to the greater demand for openness and accountability, the increase in partnership working, the desire to innovate and the greater willingness to challenge decisions.

4. Policy Statement

Policy Statement

The Council is committed to identifying, understanding and managing risks that are inherent in its services and associated service plans and strategies with a view to facilitating informed risk taking. Risk management refers to the culture, processes and structures that are directed towards effective management of potential threats and opportunities. Effective risk management optimises the balance between risk and control.

It is recognised that effective management of risk is a key element of the framework of corporate governance together with standards of conduct and service delivery arrangements. The link between the identification of key business objectives and the identification and management of key strategic risks, i.e. those risks that could have a significant adverse effect on or even prevent the achievement of these objectives, is also recognised. It is accepted that the identification and management of key strategic risks is an integral part of the service and business planning process.

It is acknowledged that, in order to be effective, risk management must operate at both a strategic and an operational level within the organisation. All staff, elected Members and those who act on behalf of the Council have a positive role to play in the management of

Appendix 1

risk. This is necessary to enable an effective assessment of risk to be undertaken when considering each policy and service delivery option available to the Council.

In seeking to manage risk, the Council will develop policies and procedures to:

- Embed risk management into the culture of the organisation;
- Raise the profile and understanding of risk management at all levels throughout the organisation;
- Develop a co-ordinated and consistent approach to the identification and management of risk throughout the organisation;
- Develop a formal, standardised risk assessment process or framework which can be applied to both current activities and new initiatives;
- Promote widespread understanding of the principles, processes and benefits of risk management via training, guidance documents etc;
- Assist each directorate in developing and recognising its own risk profile and a corporate risk register; and
- Ensure that risk is managed in accordance with best practice and in accordance with Council's approach to corporate governance.

5. Roles and responsibilities

5.1 To be effective, risk management must be adopted and incorporated as part of good management practice and operate at both strategic and operational levels within the organisation. All employees, elected Members and those who act on behalf of the Council have a positive role to play in the management of risk. This is necessary to ensure that an effective assessment of risk is undertaken when considering each policy and service delivery option available to the Council.

5.2 The principal roles and responsibilities are summarised below:-

Individual/Group	Role/Responsibility
All Members	To understand the key principles and benefits of risk management and to support the development of a corporate approach to risk management.
Standards & Governance (as the member body responsible for leading on all aspects of Corporate Governance).	To receive reports from the Audit Committee on the adequacy and effectiveness of the risk management framework

Appendix 1

<p>Audit Committee (as the Member body responsible for providing independent assurance to the Standards and Governance Committee on the adequacy and effectiveness of the risk management framework)</p>	<p>To approve the Risk Management Strategy and Policy;</p> <p>To approve, support and monitor the implementation and ongoing processes for embedding risk management throughout the Council; and</p> <p>To receive regular reports from the Chief internal Auditor (or nominated deputy) and take appropriate action to ensure that corporate business risks are being actively managed.</p>
<p>Section 151 Officer</p>	<p>To undertake the role of “Corporate Risk Champion”;</p> <p>To jointly champion, with a Member, the processes for embedding risk management throughout the Council; and</p> <p>To present reports from the Risk Management and Controls Assurance Group to the Chief Officers Management Team (“COMT”).</p>
<p>Chief Officers Management Team</p>	<p>To support and monitor the implementation and ongoing processes for embedding risk management throughout the Council;</p> <p>To consider inputs and resources required to support the strategy;</p> <p>To identify the Council’s key strategic risks to enable the Strategic Risk Register and associated “Management Action Plans” to be developed;</p> <p>To facilitate completion of and monitor progress in respect of the “Management Action Plans”; and</p> <p>To receive copies of the annual and interim reports from the Risk Management & Controls Assurance Group for noting and action as appropriate.</p>
<p>Risk Management and Controls Assurance Group</p>	<p>To focus and co-ordinate risk management activities throughout the Council and to facilitate the identification, evaluation and effective management of all key business risks;</p> <p>To raise the profile and understanding of risk management at all levels throughout the organisation;</p> <p>To develop a co-ordinated and consistent approach to the identification and management of risk throughout the organisation;</p>

Appendix 1

	<p>To promote widespread understanding of the principles, processes and benefits of risk management via training, guidance documents etc;</p> <p>To assist directorates in developing and recognising their own risk profile and to develop corporate and divisional risk registers;</p> <p>To provide a forum for risk management issues to be discussed and disseminated throughout the Council;</p> <p>To cascade information and share best practice throughout directorates;</p> <p>To support the management of risk in accordance with good practice and in accordance with Council's approach to corporate governance; and</p> <p>To support the introduction of robust business continuity plans covering key service areas and confirm that the plans are reviewed and tested within agreed timescales.</p> <p>To identify and monitor the Council's controls assurance framework and provide evidence, based on a controls self assessment process, to support the preparation of the Statement on Internal Control ("SIC").</p> <p>To present an annual report to the Audit Committee and "COMT" summarising the activities of the Group and the planned activities for the coming year.</p>
<p>Executive Directors / Heads of Service</p>	<p>To manage risk effectively in their service areas and in accordance with the agreed strategy. To support the development of Directorate Risk Registers and to ensure that they are reviewed periodically by the Directorate Management Team.</p>
<p>Risk and Controls Assurance Manager / Risk Management and Insurance Team</p>	<p>To facilitate development of the Council's risk management arrangements by providing risk management advice, training and support to Members, Executive Directors and other officers.</p> <p>To develop, maintain and communicate appropriate risk management guidance notes and documents.</p> <p>To support directorates in developing their risk management arrangements including the production of risk registers.</p> <p>To facilitate periodic review of the Strategic Risk Register in</p>

Appendix 1

	<p>conjunction with departmental Risk Champions;</p> <p>To maintain the Strategic Risk Register;</p> <p>To review and report upon the adequacy and effectiveness of the Council's risk management arrangements;</p> <p>To arrange adequate and appropriate risk financing measures and providing advice and guidance on the extent of insurance cover or self insurance arrangements;</p> <p>To provide and manage an efficient and effective insurance service for the Authority arranging, where appropriate, the placement of cover with insurers including the negotiation of premium rates and policy terms; and</p> <p>To provide and manage a claims handling service to process claims made by directorates or divisions and by members of the public.</p>
Employees	<p>To be aware of and manage risk in the course of undertaking their duties, as appropriate;</p> <p>To encourage colleagues and others to make suggestions that assist or contribute toward the effective management of risk; and</p> <p>To be aware of situations that may place themselves or others at risk and to report identified hazards.</p>
Health and Safety	<p>To ensure that health and safety risks are identified and that risk assessments are undertaken, monitored and reviewed;</p> <p>To be aware of the Council's approach to managing risk in so far it relates to health and safety; and</p> <p>To attend meetings of the "RMCAG" as the request of the Section 151 Officer.</p>
Internal Audit	<p>To facilitate the identification and management of key business risks.</p> <p>To audit and review risk management controls and processes;</p> <p>To manage the risk of fraud;</p> <p>To provide assurance to Members and senior management of the effectiveness of controls; and</p>

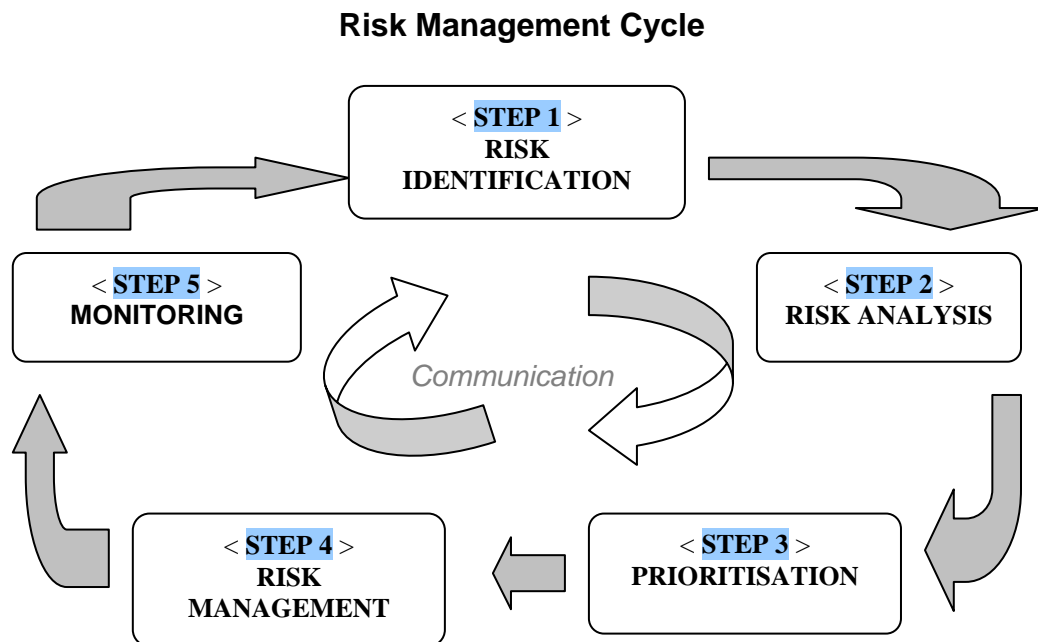
Appendix 1

	To provide advice on the identification and assessment of risks and recommend control strategies.
--	---

Appendix 1

6. Risk Management Process

6.1 In order to manage risk effectively it is necessary to develop a systematic approach to identifying, analysing and managing risk. The following diagram illustrates the risk management process that has been adopted by the Council. The process is based on good practice and is in line with the guidance contained within the Risk Management Standard Document published by the IRM, AIRMIC and ALARM:-



6.2 The first step is to identify key or significant business risks. These are risks that could have a significant adverse effect or prevent key business objectives from being met. Directorates or divisions will already, as part of the business planning process, have identified their key risks and priorities. In most cases the key business risks will therefore flow from the Business Planning document.

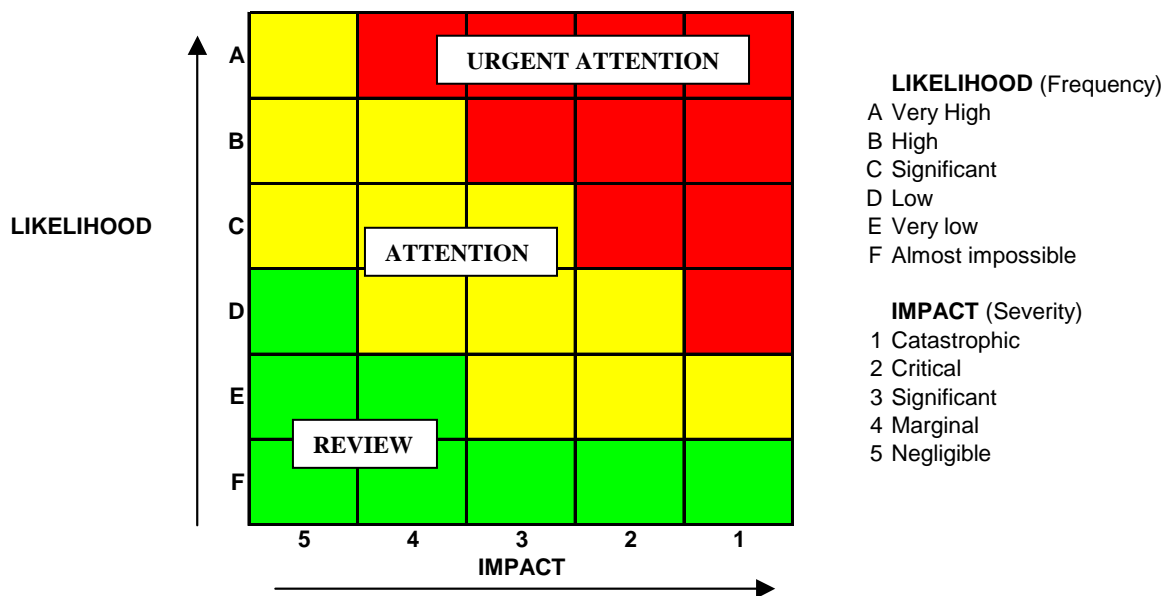
6.3 Other new or emerging risks may arise or be identified in connection with proposed partnership working arrangements or major projects. In respect of partnerships they should be reviewed in terms of risk before they are entered into. Where possible, responsibility for aspects of risk should be identified through contractual arrangements. In respect of major projects, officers nominated to manage such projects should be appropriately skilled e.g. PRINCE 2 project methodology.

6.4 The key risks can then be reviewed and an assessment made of the likely frequency (probability of risk event occurring) and severity (potential impact should such an event occur) of potential risk events should they arise. The likelihood and impact are normally based on a consensus of opinion by those officers tasked with undertaking the exercise, although other more formal risk modelling techniques could be applied.

Appendix 1

6.5 Key risks can be plotted using the following standard risk matrix. The purpose of the risk matrix is to provide a graphical representation of the risks and to assist with the prioritisation and planning process.

6.6 Prior to assessing the frequency and severity of the potential risk event, it is necessary to determine the 'risk appetite' of the directorate or division (i.e. whether it is 'risk averse' or 'risk taking'). The 'risk appetite' can then be illustrated by colour coding the relevant boxes on the risk matrix to indicate the appropriate level of response according to where a risk appears:-



6.7 It should be noted that some risks may, by their very nature, sit in the "red" zone on the basis that the risk is unavoidable and it is not within the ability of the organisation to completely manage it to a tolerable level – for example many organisations have to accept that there is a risk arising from terrorist activity which they cannot control. In these cases the organisation needs to make contingency plans.

6.8 The purpose of risk management is not to seek to drive all key risks down into the bottom left hand corner – in doing so this would mean that a directorate or division had become extremely risk averse. This would then impact on the achievement of business objectives and would stifle innovation on the basis that new initiatives or projects could only be considered if they were low risk.

For each key risk it is necessary to determine whether:-

- the risk is **accepted** – i.e. is it worthwhile to continue if the risks outweigh the reward? Certain risks may have to be accepted as they form part of, or are inherent in, the activity. It is important, however, to ensure that these risks have been identified, assessed and are clearly understood.
- the **control** strategy (i.e. the measures needed to either avoid or mitigate the risk). Can the likelihood and/or impact be 'managed down'? The control measures

Appendix 1

should, however, be commensurate with the likelihood, impact and consequence of the risk event.

- Control strategies include:-
 - **transferring** the risk by passing it onto another party via contractual arrangements
 - **eliminating** the risk by ceasing an activity
 - **sharing** the risk with another party
 - **controlling** the risk by building controls into the operational process
 - **planning** to deal with service interruption
 - **insuring** against some of the risk to mitigate the financial impact
- who is **accountable** for managing the risk (the risk owner). The risk owner should be a named individual rather than a group or committee.
- the **residual risk** - in most cases at least some actions or controls to manage the risk will already be in place. It is therefore necessary to look at these controls before considering or developing new actions or controls. After reviewing existing controls the risk may need to be 're-scored' to see whether it is still deemed to be a priority.

6.9 The outcome of the risk identification and analysis exercise needs to be formally recorded and, where appropriate, action plans developed to manage the risk (**Appendix 1**). It is important that risk registers and associated action plans are monitored and reviewed on a periodic basis to ensure that identified risks are being managed and to consider any new or emerging risks.

6.10 The normal business planning cycle will allow for the quarterly review of key risks arising from the business planning process.

7. Performance Management

7.1 A range of suitable and appropriate Key Performance Indicators ("KPIs") are to be developed by the Chief Internal Auditor and Divisional Management Team where such information can be usefully applied to develop or improve the service. The development of "KPIs" is identified as a priority within the Internal Audit, Risk and Assurance Services Business Plan.

8. Relationships with existing processes

8.1 **Corporate Governance** - This can be described as "the system by which local authorities direct or control their functions and relate to their communities. In other words, the way in which organisations manage their business, determine strategy and objectives and go about achieving those objectives. The fundamental principles are openness, integrity and accountability".

Source: Audit Commission

Appendix 1

Risk management is an integral part of good governance and serves to support the need to demonstrate an appropriate corporate culture, transparent decision-making and accountability to stakeholders.

8.2 **Corporate Priorities** - The Council published its Medium Term Plan (MTP) covering the period 2005 – 2008 which identified 5 key priorities which underpin all of Council's work. The 5 key priorities were identified using information from a range of sources including the Citizens' Panel, MORI research, community and service user feedback and complaints, Neighbourhood Partnership priorities, discussions with partners, including the Southampton Partnership, external inspections, Best Value and other reviews. The 5 key priorities are:-

- Tackling deprivation and inequalities;
- Promoting life long learning for all people;
- Improving community safety and reducing crime and disorder;
- Improving the street scene and the environment; and
- Promoting independent living.

Risk is firmly linked with the ability of the Council to fulfil its corporate objectives by developing a formal process or framework to allow key strategic and operational risks to be identified and managed. Effective risk management also supports the decision making process by facilitating informed risk taking.

8.3 **Comprehensive Performance Assessment** – The "CPA" Use of Resources includes specific and detailed reference to risk management in the "Internal Control" key line of enquiry. The "criteria for judgement" makes specific reference to the arrangements that are expected to be in place in order to secure the highest rating.

8.4 **Best Value and continuous improvement** - Risk Management and Best Value share a number of common goals:-

- they are both based on principles of quality management;
- they require a co-ordinated and integrated approach across all areas of corporate activity; and
- everyone in the chain of service needs to be involved in the process.

It can be argued that Best Value cannot be delivered unless the organisation's assets and objectives are protected. Risk Management is a system for identifying, assessing and managing all key risks that threaten the assets and objectives of the authority and so the two concepts form a valuable partnership.

8.5 **Business Planning** - There is a clear link between key business objectives and the identification and management of key business risks, i.e. those risks that could have a significant adverse effect or even prevent key objectives being met. The identification and management of key business risks, which is supported by the adoption of the EFQM Excellence Model by the Council, is therefore an integral part

Appendix 1

of the business planning process and this is reflected in the 'Corporate Business Planning Guidance'.

- 8.6 **Statement on Internal Control** - The Accounts and Audit (Amendment)(England) Regulations 2006 state that "the Council is responsible for ensuring that its financial management is adequate and effective, and that it has a sound system of internal control which facilitates the effective exercise of its functions, and which includes arrangements for the management of risk".

Regulation 4 requires the Council to conduct a review at least once a year of the effectiveness of its system of internal control and publish an annual Statement on Internal Control ("SIC") with the Authority's financial statements. Although the "SIC" is published with the Authority's financial statements it is concerned with overall internal control environment and is not confined to financial issues.

The purpose of the "SIC" is to provide a continuous review of the effectiveness of the organisation's overall internal control environment, including risk management. This requires the sources of assurance, which the Council receives, to be brought together and reviewed against the principal risks to its key objectives, with any gaps in assurance recorded and included within the "SIC".

- 8.7 **Internal Audit** - There is a clear relationship between internal audit and risk management in that the purpose of Internal Audit is to provide independent and objective assurance to the Council on risk management, control and governance, by evaluating their effectiveness in achieving the Council's stated objectives.

The relationship is particularly evident where risk registers, underpinned by a rigorous risk identification and assessment process, feed into the audit planning process.

Internal Audit will also be in a position to audit the risk management process and to assess and provide an overview of the effectiveness of risk management activity within and across the organisation.

- 8.8 **Health and Safety** - It is recognised that health and safety considerations will be an important feature in many of the key risks identified on the Corporate Risk Register and that the health, safety and welfare of all employees and Council stakeholders should be paramount. The effective management of health and safety within the Council therefore forms an integral part of the Risk Management Strategy.

An effective working relationship is maintained with the corporate Health and Safety Team.

9. Reporting

- 9.1 The "Corporate Risk Management Champion" shall present an annual report to the Audit Committee summarising achievements and outlining the planned activities for the forthcoming year as well as an interim, six-monthly report. "COMT" will also

Appendix 1

receive copies of the annual and interim reports for noting and action as appropriate.

10. Review

- 10.1 This document will be reviewed at least annually by the Council's "Risk Management and Controls Assurance Manager. Any significant changes will also be reported to the Audit Committee as the Member body responsible for providing independent assurance to the Standards and Governance Committee on the adequacy and effectiveness of the risk management framework

Appendix 1

Appendix 1

{DIRECTORATE/DIVISION/PROJECT} – RISK REGISTER

{FINANCIAL YEAR}

Key Risks

The following document represents the 'key risks' identified by the **{Management or Project Team}** on **{Date}**. This list of risks has been considered and developed based **{on the key priorities identified within the Directorate/Division Business Plan}** or **{key aims and objectives of the project}**. For each key risk there is an associated 'Management Action Plan' (MAP) which identifies a 'risk owner' and the risk management actions required.

1.0 **{Description of key risk}**

2.0 **{Description of key risk}**

3.0 **{Description of key risk}**

4.0 **{Description of key risk}**

5.0 **{Description of key risk}**

6.0 **{Description of key risk}**

Appendix 1

Appendix 1

Owned by: { **Name – Job Title** }

Last Review Date: {dd/mm/yyyy} Next Review Date: {dd/mm/yyyy}

Likelihood	A					
	B					
	C					
	D					
	E					
	F					
		5	4	3	2	1
	Impact					

Risk No.	Current Risk Score	Target Risk Score	Description of Risk Event
	[from risk matrix]	[improved position]	[description of key risk]

Ref No	Action/controls already in place	Adequacy of action/control to address risk	Required management action/control	Responsibility for action	Critical success factors & KPI's	Review frequency	Key dates
[risk should be able to be related back to key priorities or objectives]	[actions/controls already in place that relate to management of this risk]	[how effective are the actions/controls already in place?]	[new actions/controls required to manage the risk down to its target score NOTE: control may be deemed as 'Adequate' but may still require additional action to further enhance controls]	[the risk owner – NOTE: should be a named person not a Group, Mgmt Team or Committee]	[what will success look like? How will performance indicators have improved]	[frequency of review for this particular action plan]	[Milestones/ deadlines]