eastsussex.gov.uk

East Sussex County Council

Risk Management Framework

BSD Assurance
July 2015

v0.1

INVESTORS IN PEOPLE

POSITIVE ABOUT DISABLED PEOPLE

eastsussex.gov.uk

East Sussex County Council

Risk Management Framework

Summary

This framework sets out the East Sussex County Council policy on risk management and its strategy for the effective identification, assessment and, where appropriate, management of risks.

Contents

Policy Statement

a) Introduction and Objectives

The appropriate management of risk is a fundamental element of the council's ability to provide cost effective, quality services and to ultimately deliver its four priority outcomes of:

- Driving economic growth;
- Keeping vulnerable people safe;
- Helping people help themselves; and
- Making best use of our resources.

To achieve this, sound risk management policy and practice must be firmly embedded within the culture of the council, providing a proportionate and effective mechanism for the identification, assessment and, where appropriate, management of risk. This is especially important in the current climate where there remains considerable uncertainty about the future.

Robust risk management helps to improve internal control and support better decision-making, through a good understanding of individual risks and an overall risk profile that exists at a particular time. To be truly effective, risk management arrangements should be simple and should complement, rather than duplicate, other management activities.

b) Scope and Definitions

There are many definitions of 'risk' and 'risk management'. In simplest terms, these can be defined as follows:

- Risk - 'the probability of an event occurring and its consequences';
- Risk management - 'the processes and structures to enable the effective management of potential opportunities and the elimination / reduction of threats'.

Risk is unavoidable and effective risk management is not about the elimination of risk. The council's ability to manage risk effectively and proportionately, and maximise opportunity, plays a crucial role in the council's ability to achieve its business objectives. Risk management is not simply a compliance issue but is a decision making tool, utilised at both strategic and operational levels, and is therefore an essential element of effective corporate governance.

In developing this framework, the County Council recognises that risks cannot be fully managed and that, in being more innovative, efficient and effective in the delivery of its services, it may choose to take and/or accept more risk. Where this is the case, robust risk management practice will help ensure that the council takes appropriately informed decisions, having properly evaluated the potential risks and the associated opportunities.

c) Roles and Responsibilities

Members

Members are responsible for setting the strategic objectives of the council, for understanding the strategic risks it faces and satisfying themselves that appropriate action is being taken to control these risks.

The responsibilities of Cabinet include ensuring that the County Council follows best practice in relation to its risk management arrangements and it is supported in this regard by the Audit, Best Value and Community Services Scrutiny Committee, whose role includes:

- considering the effectiveness of the council's risk management processes, internal control environment and corporate governance arrangements and to recommend any changes to Governance Committee or Cabinet as appropriate;
- reviewing the council's assurance statements, including the Annual Governance Statement, ensuring that they properly reflect the risk environment, and any actions to improve it.

Corporate Management Team (CMT)

CMT are responsible for endorsing and promoting robust risk management across the organisation and maintaining and monitoring the council's Strategic Risk Register. Specifically, the role of the CMT Reconciling Policy, Performance and Resources (RPPR) Board includes 'managing escalated risk, including reputational management' and 'agreeing intervention approach when assurance is not satisfactory'.

Statutory Officers Group (SOG)

SOG is formed of the Chief Executive, the Monitoring Officer, the Chief Finance Officer, with all meetings attended by the Head of Assurance. The Chief Operating Officer also has a standing invitation and other Chief Officers and senior officers will participate and attend meetings where necessary.

The role of the group is to support CMT in fulfilling its risk management responsibilities by providing a dynamic, light touch and real time forum for considering current strategic risk and governance issues facing the organisation and ensuring that appropriate action is taken in response.

Departmental Management Teams (DMTs)

Each DMT is responsible for ensuring that risk management is embedded throughout their department and in accordance with the council's risk management framework. As part of their role, DMTs should ensure that comprehensive risk registers are maintained for their department as a whole and, where considered necessary, for individual divisions. Each DMT is responsible for reviewing these risk registers on an ongoing basis, and at least quarterly,

Service Managers

These officers are responsible for identifying, assessing and, where considered appropriate, managing risks associated with the services they deliver. This should form part of day to day management activities with risks being reviewed on an ongoing basis to ensure they continue to be relevant and that any mitigations remain effective. Regular monitoring also allows for changes in the risk profile to be assessed and emerging risks appropriately considered and controlled. This information should be recorded in departmental risks registers and reported on as part of the quarterly Council Plan monitoring process.

Corporate Risk Coordinators Group

This group is formed of risk coordinators representing each council department and is chaired by the Risk and Insurance Manager. The group supports the work of the Statutory Officers Group, and ultimately CMT, by championing and disseminating best practice within departments and acting as a facilitator of risk management activity. This is achieved through ongoing liaison with service managers to ensure the proactive identification and management of risks. Group members are also responsible for coordinating the quarterly review and updates to risk registers as part of the Council Plan monitoring process.

Risk and Insurance Manager

Provides the professional lead on risk management for the County Council, including the provision of guidance, advice and support on all risk management related issues. The Risk and Insurance Manager (RIM) also provides ongoing challenge and review of organizational risk registers, along with training to officers and Members, as appropriate.

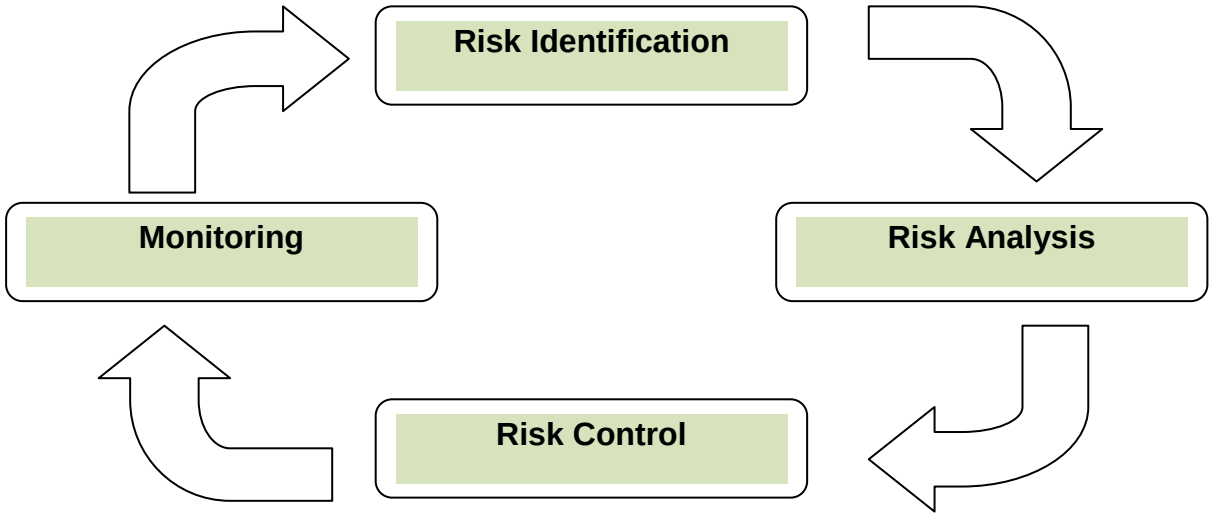
Risk Management Strategy

a) Risk Management Process

The council's risk profile is dynamic. Consequently risk management must be a continuous and developing process to ensure that the council is always in the best position to take full advantage of business opportunities, as and when they arise, and to ensure that resources are utilised to maximum benefit.

In order to appropriately and effectively manage risk, it is necessary to adopt a systematic approach to its identification, analysis and control. This approach is referred to as the 'Risk Management Process' and provides a system that can be applied to risks at all levels within the council, irrespective of risks being 'strategic' or 'operational' in nature.

The Risk Management Process



Risk information is recorded within registers maintained at a corporate (strategic) level and individual department level. In the case of some of the larger departments, divisional risk register may also be maintained. Further information on the recording, monitoring and reporting of risk is set out later in this document.

Risk Identification

The first element of the risk management process is the identification of risks. This will link in to the business planning process, where objectives and targets relating to key business activities are identified, along with associated risks. Risks associated with specific projects and partnership working should also be identified at an early stage in the planning process.

To identify risks, managers should refer to their service delivery targets / objectives and then identify threats which can potentially prevent the targets being achieved or for sub optimal outcomes to be achieved. Managers should also identify appropriate opportunities, where specific actions will result in an improved outcome beyond those originally envisaged and therefore a better return for the resources invested.

Managers should be aware that the risk profile of their service is dynamic. Risks can emerge and diminish over a relatively short period of time and therefore, it is essential that risks are reviewed on a regular basis. As a minimum, reviews must be undertaken on a quarterly basis, to match the council monitoring timetable.

Any risk identified should represent a specific threat or opportunity. Any risks that occur routinely as part of normal service delivery, and are therefore managed via normal routines and processes (e.g. service planning and performance monitoring), need not be included. The exception to this would be where the risks require escalation and/or need to be managed and monitored at a higher level.

The following represents examples of the types of risk that managers should consider. These examples are split into 'strategic' type risks and 'operational' type risks, although most services will attract risk from both categories. Also, risks are often interrelated and should not be viewed in isolation.

Strategic type risks:

Risk Category	**Definition (risks relating to…)**	**Examples**
Political	Delivery of central or local political commitments	• Inability to deliver strategies • Inability to meet expectations
Economic / Financial	Ability to meet the council's financial commitments	• Missed business opportunities • National / regional economic issues • Funding / budgetary deficit • Lack of investment
Social / Service delivery	Impact on service delivery due to social factors	• Crime and disorder • Demographic changes such as aging population
Technological	Impact of technology on service delivery	• Major, long-term loss of IT systems • Inability to deal with changing technological demands • Obsolescence
Environmental	Risk relating to environmental factors	• Impact of planning and transport policies • Pollution • Environmental change

Risk Category	Definition (risks relating to…)	Examples
Legal / compliance	Changes to UK / EU law / guidance	• Inadequate response to legislative change • Breaches of the law • Inability to comply with requirements / guidance
Customer	Changing needs / expectations of customers	• Failure to meet stakeholders needs.
Reputation	Risks relating to the council's reputation.	• Loss of image • Failure to enhance the council's image • Adverse publicity

Operational type risks:

Risk Category	Definition (risks relating to…)	Examples
Financial	Risk associated with financial planning, control and the adequacy of internal funds. Alterations to external funding	• Poor internal financial control • Missed funding opportunities • Fraud and corruption • Funding shortfall
Professional / Managerial / staff	Risks associated with professional and management issues	• Failure to recruit and retain professional staff • Poor management practice • Poor service provision • Loss of key staff
Physical	Risks related to material damage, health and safety, security	• Loss of / damage to assets • Non-compliance with work place / Health & Safety legislation.
Environmental	Risks relating to pollution, noise, energy efficiency	• Noise • Contamination • Pollution
Contractual / Partnership / Supply chain	The failure of a partner / contractor / supplier to meet obligations or expectations	• Over reliance on a key supplier • Failure of a partner to deliver service to an acceptable standard
Technological	Risks relating to ICT or other systems	• Loss of ICT systems • Spread of computer virus • Hacking

Risk Articulation

In order to help understand the significance of a risk and to identify the most appropriate mitigating actions, it is important that each risk is articulated in a way that clearly identifies the nature of the risk. If possible, the type / category into which the risk falls (see above) should be identified. Also the potential impact and consequences should be included in the risk description i.e. if the risk event occurs, what will be the impact on the council and the ability to deliver the service in question?

Risk Analysis

Once risks have been identified and articulated they should be assessed in terms of:

- The likelihood / frequency of the identified event occurring i.e. how likely is it that the identified risk event will occur and / or how often?
- The severity / impact should the identified event occur i.e. if the identified risk event does occur, how severe are the consequences?

Both 'likelihood' and 'severity' should be scored from '1' to '4' with 1 being the lowest. When these scores are placed on the risk matrix (likelihood x severity), this will produce an overall risk score for each risk, from '1' to '16'. These scores fall into 3 categories.

- LOW risks (Green) = Risk score 1 – 3
- MEDIUM risks (Amber) = Risk Score 4 – 8
- HIGH risks (Red) = Risk score 9 - 16

		IMPACT			
LIKELIHOOD		**Low 1**	**Medium 2**	**High 3**	**Extreme 4**
Unlikely	1	1 (Low)	2 (Low)	3 (Low)	4 (Medium)
Moderate	2	2 (Low)	4 (Medium)	6 (Medium)	8 (Medium)
Likely	3	3 (Low)	6 (Medium)	9 (High)	12 (High)
Almost certain	4	4 (Medium)	8 (Medium)	12 (High)	16 (High)

The scoring of both likelihood and impact will rely on each manager's knowledge of their own service and will vary depending on the nature of the risk, with an inevitable element of professional judgement involved. However, a rough guide is as follows:

Likelihood:

Unlikely (1): The event is unlikely to occur and historically has only occurred on rare occasions.

Moderate (2): There is a reasonable chance that the risk event will occur, although it can still be considered unlikely.

Likely (3): The risk event is more likely to occur than not. There is a reasonable chance of the risk event occurring.

Almost certain (4): The risk event is highly likely to occur and the chances of it not occurring are minimal.

Impact:

Low (1):	Minor service disruption / minimal budgetary impact/ isolated customer complaints / minimal impact on key objectives.
Medium (2):	Noticeable service disruption / injury resulting in loss of work time / more serious budgetary impact / adverse local media coverage / many customer complaints / noticeable impact on key objective.
High (3):	Significant service disruptions / serious injury / significant budgetary impact/ adverse national media coverage / attainment of key objectives rendered difficult.
Extreme (4):	Total service loss for a significant period / fatality or multiple serious injuries / loss of 50% or more of budget / Governmental or regulatory body intervention / attainment of key objective rendered impossible.

Once the overall risk score has been calculated and the risk allocated a 'RAG' rating (Red, Amber, Green), appropriate risk control/mitigation measures should be identified.

Risk Control

The aim of risk control is not to remove or avoid all risks, since this would be indicative of a 'risk averse' culture and would not enable the organisation to benefit from innovation and new, untried initiatives. It is also important to recognise that, by their nature, some risks will remain significant, irrespective of the control measures put in place, because they may be beyond the powers of the council to control.

The key to effective risk control is ensuring that a proportionate and cost effective approach is taken, having regard to the level of actual risk exposure and the benefits to be obtained. As a general rule, the cost of controlling a risk should not exceed the cost to the council should the risk materialise. There are various strategies which can be taken in response to an identified risk and these include:

- **Terminate** – avoid the risk altogether by ceasing the activity to which the risk relates. This tends to be adopted where the level of risk is extreme and where there is little opportunity to control it cost effectively. This option may often be unavailable to the County Council, especially in areas where we have a statutory duty to deliver a service;
- **Treat** – mitigate or control the risk. Involves implementing actions aimed at reducing either the impact or likelihood of the risk, recognising these actions should not be in excess of the level of risk exposure in terms of cost or resources;
- **Tolerate** – accept the risk, without any mitigations, based on the potential rewards outweighing the level of risk exposure. This approach tends to be used most often where the rewards or the costs of mitigation are especially high;
- **Transfer** – achieved through the use of insurances or payments to third parties who are prepared to take on the risk as part of a contract. This approach is, however, unlikely to reduce any reputational risk to the council.

Whilst all of these strategies are available, there will be some areas of risk which the council will not tolerate and will always seek to reduce to an acceptable level. These areas are based on the council's **risk appetite** which is defined as 'the amount of risk an organisation is willing to accept'. This is a determination which will vary between organisations and in the case of ESCC, will be subject to ongoing consideration by Members and CMT. Currently, the following areas are deemed to have the lowest tolerance levels i.e. where the council is prepared to accept very little risk:

- Complying with the law;
- Health and safety of service users and staff.

Where a decision is taken to mitigate or control a risk (treat), the measures taken should be appropriate and proportionate based on the likelihood, impact and potential consequence of the risk event. The nature of control risk strategies will therefore vary depending on the nature of the identified risk. Some control measures will address the likelihood element of the risk (i.e. reduce the likelihood of the risk event occurring) while others will address the impact element (i.e. once the event has occurred they will reduce the potential harm caused by the risk).

Even where it appears that an identified risk is outside the scope of meaningful control (such as the impact of severe weather events), a regularly reviewed and tested contingency plan will help reduce the detrimental impact.

Control measures will usually constitute some form of positive action and may therefore also form part of organisational service plans. By recording them in this way, targets can be set against the risk controls which can then be subject to ongoing monitoring and review as part of already established management processes.

Post Mitigation Scoring

Once mitigating actions are identified, each individual risk should be re-scored, in terms of both impact and likelihood, using the same scale (1-4) as noted above. This will result in each risk being allocated a 'post mitigation' risk score, and associated RAG rating.

The purpose of post mitigation scoring is to assess the effectiveness of the control measures at reducing either the impact or the likelihood element of the risk, thereby illustrating the level of remaining or 'residual' risk. Should this remain unacceptably high, management should consider whether further mitigating measures are required.

b) Monitoring and Reporting

The Council's risk profile is dynamic and continually changing due to the influence of external factors and / or internal influences. The level of risk can alter and consequently, identified risks and associated mitigations should be periodically re-assessed by management to address and combat the impact of these changes. In addition to this, new risks will periodically emerge which must be identified and analysed as quickly as possible to either reduce the council's exposure to adverse risk or enable the it to take advantage of business opportunities, as they arise.

As a minimum, all risk registers should be formally reviewed and updated on a quarterly basis as part of the Council Plan Monitoring. This process should include a review of departmental risk registers by each DMT, including any strategic risks for which the Chief Officer concerned has responsibility, prior to subsequent review by CMT. At the same time, the Strategic Risk Register is also reviewed and updated by CMT prior to being reported to Cabinet Committee and the Audit, Best Value and Community Services Scrutiny Committee. This process is administered by departmental risk co-ordinators, with support from the Corporate Performance Team and the Risk and Insurance Manager.

As part of the above process, consideration must be given as to the escalation and de-escalation of risks between the Departmental and Strategic Risk Registers. This is particularly important for ensuring that:

- Responsibility for any mitigating actions rests with the appropriate officers, and;
- There is sufficient awareness within the organisation of potential exposures for monitoring and decision making purposes.

The Risk and Insurance Manager will provide ongoing advice, support and challenge on risk management matters and on the content of risk registers throughout the year. Periodic training and awareness sessions will also be made available to managers.

c) Project and Programme Risk Management

The principles and approach to risk management set out within this framework should be applied equally to all council projects and programmes. Individual risk registers should be maintained for each project/programme which should be subject to regular monitoring, review and reporting as part of the established project governance arrangements.

It is the responsibility of project/programme boards to ensure that these arrangements are in place and that risks are being appropriately managed. Where project or programme risks are deemed to be sufficiently significant or where they cannot be effectively managed within the project/programme structure, these should be escalated to either departmental risk registers or the council strategic risk register.

d) Conclusions

The appropriate management of risk is a fundamental element of the council's management process, and is essential if the organisation is to successfully deliver its objectives. The aim of this Framework is to provide guidance on the risk management process and to assist with the further embedding of risk management within the culture of the council.