Management of Risk Policy Pathway

2019

Senior Responsible Owner	P Flaherty, CEO	1st October 2019
Author	P Pursley, Strategic Risk Manager	September 2019
Quality Assurance	Strategic Risk Management Group	September 2019
	Governance Board	September 2019
Final copy sign off	Senior Leadership Team	1st October 2019
Adopted into the business	Cabinet	December 2019

Pathway

INTRODUCTION

This risk management Policy and supporting documentation supports the Council in the effective management of its risk. In implementing our Management of Risk Pathway, of which this document is a part, we seek to provide assurance to all our stakeholders that the identification and management of risk plays a key role in the delivery of our strategy and related objectives.

The Council will involve, empower and give ownership to all our staff in the identification and management of risk. Management of risk activity will be regularly supported through discussion and appropriate action by senior management. This will include a thorough review and confirmation of the significant risks, those with a current score of 16 or more, evaluating their mitigation strategies and establishing supporting actions to be taken to reduce them to an acceptable level.

Though this policy the management of risk will be an integral part of both strategic and operational planning.

Risk management processes shall be structured to include:

- Risk identification and assessment to determine and prioritise how the risks should be managed;
- The selection, design and implementation of risk treatment options that support achievement of intended outcomes and manage risks to an acceptable level;
- The design and operation of integrated, insightful and informative risk monitoring and
- Timely accurate and useful risk reporting to enhance the quality of decision-making and to support management and oversight bodies in meeting their responsibilities.
- Risk management shall be an essential part of **governance and leadership**, and fundamental to how the organisation is directed, managed and controlled at all levels.
- Risk management shall be an **integral** part of all organisational activities to support decision-making in achieving objective.
- Risk management shall be **collaborative and informed** by the best available information.
- Risk management shall be **continually improved** through learning and experience

The Purpose of the risk management policy

1.1.1 This policy is intended to provide a framework for the management of risk and to increase overall awareness of risk throughout the council. The policy is to

 **denotes an update or addition to the policy and process**

empower and enable managers and those responsible for risk reporting, to better identify, assess and control risks within their areas

This risk management policy is a formal acknowledgement of the commitment of the Council to managing its risks. This policy statement will include:

- What is not covered by this policy
- The rationale for risk management
- Roles and Responsibilities of employees
- Arrangements for embedding risk management
- Sign off by CEO.

This Policy is integral to many of the Councils documents, including:

- Corporate Governance Framework
- Annual Governance Statement
- Medium Term Financial Plan (MTFP)
- Value for Money Strategy
- Healthy Organization
- Performance Management Framework
- Strategic and Service Planning
- Commissioning Gateway
- Corporate Business Continuity Plan
- Health & Safety Policy
- Information Governance

What isn't covered by this policy

This policy does not cover:

- The day to day risks around safeguarding or care of vulnerable individual children or adults. Local arrangements and policies will be in place for these types of risks.
- The threats that are covered by the Councils Health & Safety Policy.

The rationale for risk management

Risk management is a vital activity that both underpins and forms part of our vision, values and strategic objectives, including those of operating effectively and efficiently as well as providing confidence to our community. Risk is present in everything we do, and it is therefore our policy to identify, assess and manage the key areas of risk on a pro-active basis.

The Council's risk management aims are

1. To be proactive and ensure risks are identified early and managed effectively
2. To ensure the council is risk aware not risk averse

 **denotes an update or addition to the policy and process**

3. To enable the council to invest in risk prevention
4. To ensure that the council's policies, strategies, service planning, financial planning and management and its decisions making process consider risks and the appropriate mitigations
5. To acknowledge that talking about risk does not stop innovation or the things we need to do

The Council's risk management objectives are:

1. Establishing clear roles, responsibilities and reporting lines for risk management across the Council
2. Developing, documenting and implementing an approach to risk management that is consistent with current best practice and embraces all forms of service delivery, including collaborative arrangements
3. Raising and maintaining awareness of risk management with elected members, staff, partners, providers and contractors to develop a common understanding of the Council's expectations with regard to risk management
4. Integrating risk management with corporate, service and other business and financial planning processes
5. Providing a robust and systematic framework for identifying, managing, responding to and monitoring risk
6. Managing risk to an acceptable level through appropriate mitigations and prioritising the use of its available resources
7. Providing assurance, through risk reporting, of a robust management system for evidencing appropriate risk management
8. Using risk management key performance indicators to measure the effectiveness of risk management activities and the implementation of this policy
9. Benchmarking our risk management performance by reference to the CIPFA/ALARM risk management maturity model, and defining an acceptable level of performance

By having in place an effective process for managing threats and a clear escalation process that ensures problems will be dealt with at an early stage before they become a potentially significant issue. The Council also recognises, however, that risk management is about exploiting opportunities as it is about managing threats, whilst recognising that risks are inherent in all that we do. A full risk assessment should be conducted to assess the level of risk versus the opportunity to be gained. Risks need to be managed rather than avoided, and consideration of risk should not stifle innovation. In some cases, the Council may wish to accept a relatively high level of risk because the benefits of the action outweigh the risk or disadvantages on the basis that the risk will be well managed.

 **denotes an update or addition to the policy and process**

MANAGEMENT of RISK PROCESS PATHWAY

This Policy cross-references to the Management of Risk Process Pathway document which, describes the terms and steps to the identification of business risks and when the process will be applied.

Risk Assessment Matrix

The risk assessment matrix is a 5 x 5 grid that guides users through the priority scoring of individual risks and therefore which risks need to be managed via JCAD. See Appendix A for the amended Risk Assessment Matrix.

Risk Response

Risks that are important and/or urgent enough to warrant investigation in action must be responded to in the optimal way. Risk response planning enables a range of response options to be considered.

- **Terminate**: Remove the cause of the threat, cease activity
- **Treat**: Put in place mitigation to reduce the likelihood or impact, making it less likely to have a severe impact on the Council if it materialized
- **Transfer** the risk: Pass the whole risk to a third party
- **Tolerate** the risk: The Council accepts the chance the risk may occur but has the resources/capacity to deal with it if it did.

JCAD Core®™

JCAD is the Councils risk management system for recording, monitoring and reviewing those risks that require a management response. The Risk Assessment Matrix (Appendix A) sets out the Councils appetite for the recording of risks in JCAD. **Managers note: any risk report generated from JCAD has a retention period of six years from the date printed on the report.** Risk assessments are necessary for the following;

Service Area	Recording mechanism	Responsibility lies with …
BAU: Service Planning risks, Service lead project risks, Commissioning & Procurement risks Risks from Key decisions	JCAD	**Individual Strategic & Service Managers** to identify risks, appropriate owners, current and new controls. To review regularly and update when prompted. **Senior Risk Owner:** To ensure controls

denotes an update or addition to the policy and process

Service Area	Recording mechanism	Responsibility lies with …
		are being managed to have a positive effect on the risk. And is responsible for the update of the "Current Score" at each review.
Strategic Risks	JCAD	**All Corporate Directors** with assistance of the Strategic Risk Manager. Identify existing and new controls with appropriate owners.
Corporate Programme & projects inc. Business Change and Innovation projects	JCAD	Programme & Project officers/managers to identify risks, appropriate owners, current and new controls.
Internal Audit Partial Recommendations	JCAD	Strategic & Service Managers.

Notifications: An automatic notification timeline is established once a record has been created in JCAD. This generates an email reminder to the risk / and or control owner when a review is due. If the review does not take place, repeat emails will be sent fortnightly until reviews have been completed.

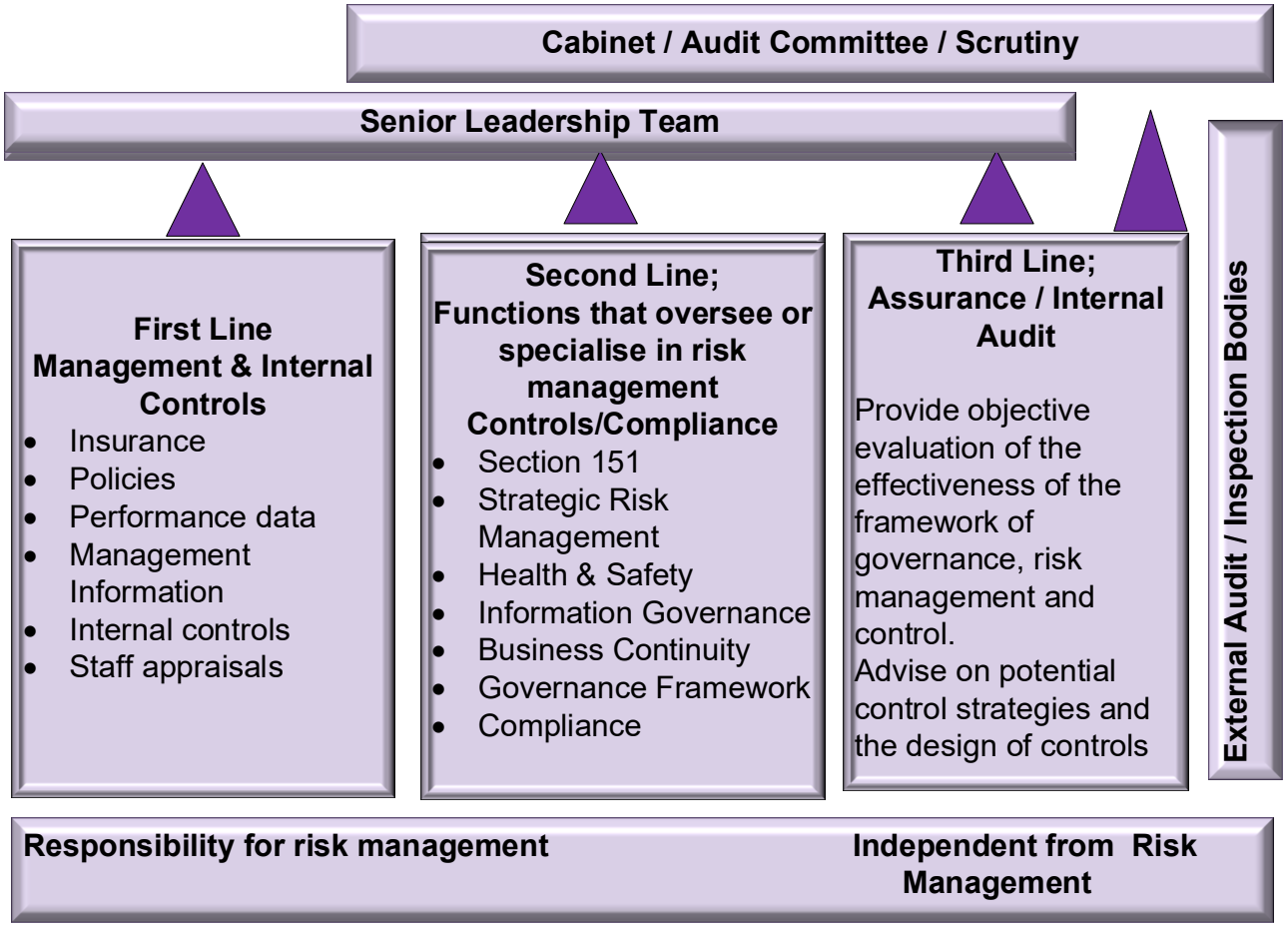
Controls: You are required to identify the existing control measures for each risk, if this does not provide adequate assurance then new controls will need to be added. All need to be recorded in JCAD, existing controls do not need further monitoring, so ownership & review dates are not necessary. Newly identified controls do need an individual owner who is responsible for the regular monitoring and review of the control, a maximum of a quarterly review period to coincide with the date of the review by the Senior Risk Owner (SRO).

Senior Risk Owner: Each risk must have an individual Senior Risk Owner. For Strategic Risks this will be a Director for BAU risks and programme / project risks this will be a Service Manager or above. The SRO is responsible for ensuring that all controls are appropriate and will have a positive effect on the risk, and on review, the SRO is responsible for the review of the "Current Score".

denotes an update or addition to the policy and process

Three Lines of Defense

All members of staff within the Council have some responsibility for risk management. A concept for helping to identify and understand the different contributions various sources of assurance can provide is the Three Lines of Defense model. By defining the sources of assurance in three broad categories, it helps to understand how each contributes to the overall level of assurance provided and how best they can be integrated and mutually supportive.
For example, management assurances could be harnessed to provide coverage of routine operations, with internal audit activity targeted at riskier or more complex areas.



First line of defence

Under the "first line of defence", management have primary ownership, responsibility and accountability for identifying, assessing and managing risks. Their activities create and/or

denotes an update or addition to the policy and process

manage the risks that can facilitate or prevent an organisation's objectives from being achieved.

The first line 'own' the risks and are responsible for execution of the organisation's response to those risks through executing internal controls on a day-to-day basis and for implementing corrective actions to address deficiencies. Through a cascading responsibility structure, managers design, operate and improve processes, policies, procedures, activities, devices, practices, or other conditions and/or actions that maintain and/or modify risks and supervise effective execution. There should be adequate managerial and supervisory controls in place to ensure compliance and to highlight control breakdown, variations in or inadequate processes and unexpected events, supported by routine performance and compliance information.

Second line of defence

The second line of defence consists of functions and activities that monitor and facilitate the implementation of effective risk management practices and facilitate the reporting of adequate risk related information throughout the organisation. The second line should support management by bringing expertise, process excellence, and monitoring alongside the first line to help ensure that risk is effectively managed.

The second line should have a defined and consistent approach to assurance that aims to ensure standards are being applied effectively and appropriately. This would typically include compliance assessments or reviews carried out to determine that standards, expectations, policy and/or regulatory considerations are being met in line with expectations across the organisation.

Third line of defence

Internal audit forms the organisation's "third line of defence". An independent internal audit function will, through a risk-based approach to its work, provide assurance over how effectively the organisation assesses and manages its risks, including assurance on the effectiveness of the "first and second lines of defence". It should encompass all elements of the risk management framework and should include in its potential scope all risk and control activities. Internal audit may also provide assurance over the management of cross-organisational risks and support the sharing of good practice between organisations, subject to considering the privacy and confidentiality of information.

 **denotes an update or addition to the policy and process**

External assurance

Sitting outside of the organisation's risk management framework and the three lines of defence, are a range of other sources of assurance that support an organisation's understanding and assessment of its management of risks and its operation of controls, including:

- external auditors, chiefly the National Audit Office, who have a statutory responsibility for certification audit of the financial statements;
- value for money studies undertaken by the NAO, which Parliament use to hold government to account for how it spends public money; and
- the Infrastructure and Projects Authority (IPA), who arrange and manage independent expert assurance reviews of major government projects that provide critical input to HM Treasury business case appraisal and financial approval points.

Other sources of independent external assurance may include independent inspection bodies, external system accreditation reviews/certification (e.g. ISO), and HM Treasury/Cabinet Office/ Parliamentary activities that support scrutiny and approval processes.

Careful coordination is necessary to avoid unnecessary duplication of efforts, while assuring that all significant risks are addressed appropriately. Coordination may take a variety of forms depending on the nature of the organisation and the specific work done by each party. It is likely to be helpful to adopt a common assurance 'language' or set of definitions across the 'lines of defence' to ease understanding, for example, in defining what is an acceptable level of control or a significant control weakness.

Roles and Responsibilities

It is the responsibility of the Senior Management Team (SLT) to ensure that the Risk Management Framework is implemented consistently across the Council.

All members of staff have a responsibility to support and embed this policy, to identify and escalate risks and to demonstrate consideration of risks in support of proposals and/or decisions.

Chief Executive Officer

Responsible for establishing the overall risk management framework

- Make decisions with proper consideration to risks
- Approves the strategy, business plans and budgets based on the risk management information

 **denotes an update or addition to the policy and process**

- Allocate responsibility for effective risk management to risk owners
- Assign responsibility for designing and implementing the risk management pathway to the Strategic Risk Manager
- Allocate resources necessary to perform business activities with risks in mind

Senior Leadership Team

- Responsibility for the setting of the Councils risk appetite and tolerance levels
- Drive the SLT agenda by discussing those areas that are most at risk
- Provide oversight of the overall risk management effectiveness, including standards and values
- Make Board level decisions with proper consideration to risks and guidance
- Review and establish risk appetites/limits for certain business activities, types of risks (usually required by law) or decisions
- Set risk-adjusted performance targets and KPIs for CEO and the management
- Responsibility for risk management lies with service directors and management teams, and failure to keep risks updated will be an indicator of performance issues;

Individual Directors

- Are responsible, with their individual management teams, to identify the top risks for their Directorate
- To ensure those risks are entered onto JCAD and that regular monitoring and review takes place.
- Are responsible for the monitoring of partial audit recommendations resulting from Internal Audit reports, these are recorded in JCAD.
- Responsibility for risk management lies with service directors and management teams, and failure to keep risks updated will be an indicator of performance issues;

Strategic Risk Manager

- Author of the Councils Risk Management strategy, policy and process documents
- Advise Senior Officers on the implementation of the risk management pathway
- Coordinate risk management activities and provide methodological support for the risk-based decision making
- Participate in the preparation of management reports for strategic and the top directorate risks
- Coordinate the work of the Strategic Risk Management Group
- Provide risk management training
- Author eLearning materials
- Implement activities designed to integrate risk management into the overall culture of the organisation

 **denotes an update or addition to the policy and process**

Strategic Risk Management Group

- Quality Assurance of the Management of Risk Pathway suite of documents
- Monitor existing and suggest, emerging strategic risks to senior leadership team

Strategic and Service Managers

- Identify, assess and treat risks associated with business activities or decision-making within their area of responsibility
- Includes a responsibility for service management teams to include risk management as a regular agenda item for their meetings;
- Allocate resources necessary to manage risks within their area of responsibility
- Optimise business processes or decision making based on the information about risks.
- Are responsible for the monitoring of partial audit recommendations resulting from Internal Audit reports, these are recorded in JCAD.
- Ensure that all service level and project risks are entered onto JCAD and that regular monitoring and review takes place.
- Discuss the risks for their service area at management meetings to gain assurance that the risks are being managed down to an acceptable level.
- Ensure risk is part of finance and performance reporting

Risk Escalation

 All officers are responsible for the identification and management of risks. Where a risk moves beyond the control of an individual service or is above your target level of risk, the risk should be escalated by the senior manager to the Corporate Director, discussions around risk should be a standard agenda item on all management team meetings to enable this to happen and identify who has the authority and the accountability to authorise additional resources to control the risk. Escalation enables the transferring of ownership and accountability, up through the escalation route outlined below. Escalation does not necessarily mean that the risk will be adopted at a higher level e.g. Directorate or strategic, it does enable approval for additional mitigation at a higher level.

 **denotes an update or addition to the policy and process**

Escalation of a risk						
	Service Manager	Strategic Manager	Service/ Corporate Director	Senior Leadership Team (SLT)	Audit (A) and/or Scrutiny Committee	Cabinet
Service Level	√	√	√			
Directorate Level			√	√	√	√
Strategic Level				√	√	√
Programme & Project Risks						
	Project & Change Officer	Project & Change Managers	Project Board	Programme Manager	Programme Board	
	√	√	√	√	√	

Risk financing

There are several options for financing the management and materialisation of risks to the Council and its services. The most obvious of these is through conventional insurance, which serves to reduce the financial effect of low likelihood plus high impact events, although this will apply to only 20 percent of risks identified. Other options include spending on actions to lower the level of risk. This is more likely to occur in respect of operational risk, where controls can more readily be implemented. For example, spending on security to reduce the incidence of theft.

As part of the annual budget setting process, the Council also sets its contingency budget. This specific annual revenue budget allocation is also a means of potentially funding risks that are unable to be controlled by mitigations and or exceed tolerance e.g. the consequences of an extreme weather event or legal actions against the council.

RISK REPORTING

When risk reporting, you maintain the ownership and the accountability for that risk, and informing senior leadership of the current situation, so they can make risk informed decisions. We report risks from the following;

- Service level risks

denotes an update or addition to the policy and process

- Directorate level risks
- Strategic risks
- Programme & project risks which are the responsibility of the Programme Office.

- JCAD Core provides the standard reporting template (JCAD/Report Explorer/Business Unit Risk Report) used across all services and projects.
- Risk should also appear on individual services / Directorate performance score cards

Risk Reporting						
	Service Team Meetings	Strategic Manager Team meetings	Directorate Management meetings	Senior Leadership Team (SLT)*	Audit Committee	Cabinet
Service Level	√	√	√			
Directorate Level		√	√	√	√	
Strategic Level				√	√	√
Internal Audit Reports	√	√	√	√	√	
Programme & Project Risks						
	Project & Change Officers	Project & Change Managers	Project Board	Programme Manager	Programme Board	
		√	√	√	√	

*Any risks overdue for a significant period, will be immediately escalated to SLT for discussion.

Reporting Frequency

Recipient	**Frequency**	**Format**
Cabinet	Annual	Report on Risk Management Policy and Strategy, together with Council Risk Report
Cabinet	Quarterly	As part of Corporate Performance Report
Scrutiny	Quarterly	As part of Corporate Performance Report
Audit Committee	Quarterly	Report on Strategic risks with a

 **denotes an update or addition to the policy and process**

		focus on the controls. Report on the Internal Audit Partial Audit Recommendations
SLT	Quarterly	Report on Strategic risks & escalation of out of tolerance commissioning / business risks and emerging risks
SRMG	Monthly	Strategic Risk Report Escalation reporting to SLT Identification of emerging risks Quality Assurance of the MoR Pathway documents
Governance Board	Monthly	Review Risk Management compliance as part of SCCs Assurance Framework

Committee Reports and Decision reports: Report templates contain a section on 'Financial/Risk Implications' which officers are required to consider and complete when writing.

Significant risks identified by risk assessment should be noted here (i.e. those assessed as being 'high' when applying the Council's risk assessment criteria). High risks should also be referred to in the main body of the report, together with any further measures proposed to control the risk.

- When/if the decision is approved a formal risk assessment should be carried out and the results entered into JCAD for monitoring and review.

5.2. Strategic Risk Management Group (SRMG)

SRMG meet monthly, is chaired by a Corporate Director and has attendees from technical risk management functions from across the council, along with representatives from services. SRMG provide a quality assurance role for the MOR Pathway documents.

SRMG also have an assurance role in establishing compliance with strategy and provide a 'critical friend' role to services. Where necessary SRMG will escalate out of tolerance risks to SLT for recommended management action.

SRMG have the option of 'calling in' a risk owner to discuss any risk that has seen no or little improvement, or a risk that has escalated to be out of tolerance.

denotes an update or addition to the policy and process

SRMG reports directly to SLT at their Business meetings. Reports also include any emerging risks suggested by Directors or services for SLT's consideration, the latest performance data compiled from JCAD Core and areas of concern SRMG may have.

 **denotes an update or addition to the policy and process**

Risk Reporting timescales

Combined likelihood x impact score	**Reporting timeframe**
Very High (Red)	Monthly – record in JCAD
High (Orange)	Monthly – record in JCAD
Medium (Yellow)	Quarterly – record in JCAD
Low (Green)	At least annual – recording in JCAD is voluntary, but you must record and monitor somewhere, perhaps in your Commissioning/Service Plan template.
Very Low (Green)	At least annual – recording in JCAD is voluntary, but you must record and monitor somewhere, perhaps in your Commissioning/Service Plan template.

Training and awareness

Member training has been targeted to Audit Committee, the Cabinet and as part of the Member Development Programme.

Training for Strategic Managers and Service Managers is provided to prepare them for risk assessment of their services and raise awareness of what is required of them in relation to risk management.

Embedding risk management into organisational culture and business processes
Staff involvement

For the risk management process to become fully embedded, it is important that all staff across the organisation are engaged within it. This will be achieved through:

- Including risk management discussions during staff appraisals and supervision
- Involving staff in the process of identifying the risks from within their area of work / service.
- Targeted training and support opportunities for all staff
- E-learning module via the Learning Centre

denotes an update or addition to the policy and process

Directors, strategic and service managers should;

- Play an integral part in the identification, assessment and management of the range of risks they are exposed to which, may threaten the successful delivery against identified objectives.
- Set feasible and affordable strategies and plans
- Evaluate and develop realistic programmes, projects and policy initiatives
- Prioritise and direct resources and the development of capabilities
- Identify and assess risks that can arise and impact the successful achievement of objectives
- Determine the nature and extent of the risks that the organisation is willing to take to achieve its objectives
- Design and operate internal controls in line with good practice
- Deliver innovation and incremental improvements.

 **denotes an update or addition to the policy and process**