Suffolk County Council

# CORPORATE RISK MANAGEMENT STRATEGY

(Last updated: Paul Emeny 16th June 2026)

*Why managing risk is important?*

It is universally recognised that managing risk is an essential part of good governance within any organisation and is intended to be a business-as-usual process that enables an organisation to manage uncertainty in a systematic and consistent way. Risk management supports informed decision making thereby enabling opportunities to be considered or action taken to mitigate risks to an acceptable level.

*Approach to Managing Risk*

The Council follows an 'Active Risk Management' approach to managing its risks, a flexible and common-sense framework with a focus on actively identifying the likelihood of something happening, and, if that 'something' did happen, what impact would it have on the organisation's ability to deliver its priorities. This approach aligns to the revised Chartered Institute of Internal Auditors 'Three Lines Model', a model that promotes the delegation of risk management roles and responsibilities across the organisation.

Risk management is a key element of the Annual Governance Statement, a process that is reviewed annually to ensure the Council is meeting the principles of its Code of Corporate Governance in accordance with CIPFA (Chartered Institute of Public Finance and Accountancy) and SOLACE (Society of Local Authority Chief Executives) Framework 'Delivering Good Governance in Local Government'.

Risks are first identified, then assessed/scored, and assigned to a risk owner, usually a senior manager who is then responsible for regularly monitored and reviewing the risk and managing any specific actions put in place to help mitigate the risk. All high level risks are held on a risk register and then reported to senior leadership teams for oversight and taking the necessary action where this is deemed necessary. Senior leaderships teams include both Corporate and Directorate Leadership Teams, as well as Cabinet and Audit Committee. Generally, risk registers are monitored at a senior level every quarterly, but less/more frequently if there is a business need to do so.

The Primary purpose of managing risks in this way is to:

| | |
|---|---|
| Provide leadership teams with visibility, oversight, and a clear understanding of the active risks being managed by the Council. | Opportunity for cross-departmental challenge and effective use of organisational resources. |
| Enable issues to be identified and appropriate action taken through the relevant management team. | Provides accountability and transparency. |

Generally, the reporting of risk registers is undertaken alongside other management activities such as finance and performance monitoring. High-level risks are usually categorised and themed in alignment with best practice and industry standard frameworks. For example, Suffolk County Council categorises all its high-level risks into three broad areas:


In principle a corporate level risk is one that would significantly impact on the Council's ability to achieve its priorities or something that would impact on the whole organisation.

- A risk could adversely affect the corporate governance of the Council.
- A risk could impact on all parts of the organisation.
- A risk has the potential to affect the achievement of corporate priorities.
- A risk could inflict major reputational and/or financial damage on the Council.

Risks deemed to be 'corporate' (the highest) level are usually allocated an Assistant Director or above to control and manage the risk until such time as it is downgraded to a lower level or withdrawn.

Strategic level risks are also things that would have a significant impact on delivering services but are generally things are can be contained at directorate level rather than organisational. 'Operational' risks usually have potential to impact specific services. All corporate level risks are reported at the highest level of management as are some strategic risks. Operational level risks are generally managed within the relevant service area.

All risks are then grouped into standardised themes that best describe the source of the risk to facilitate the identification of common issues and helps the Council create an overall risk profile.

| | |
|---|---|
| Governance risks | Risks arising from plans, priorities, and accountabilities, and/or ineffective or disproportionate oversight of decision making and/or performance. |
| Legal risks | Risks arising from a defective transaction, a claim being made, or some other legal event occurring that results in a liability or other loss, to take appropriate measures to meet regulatory requirements or to protect assets. |
| Financial risks | Risks arising from not managing finances in accordance with requirements and financial constraints resulting in poor returns from investments, failure to manage assets/liabilities or to obtain value for money from the resources deployed. |
| Property risks | Risks arising from property deficiencies or poorly designed or ineffective/ inefficient safety management resulting in non-compliance and/or harm and suffering to employees, contractors, service users or the public. |
| Commercial risks | Risks arising from weaknesses in the management of commercial partnerships, supply chains and contractual requirements, resulting in inefficiencies, fraud, and /or failure to meet business requirements/objectives. |
| People risks | Risks arising from ineffective leadership and engagement, inappropriate behaviours, the unavailability of sufficient |

| | |
|---|---|
| | capacity and capability, industrial action and/or non-compliance with relevant employment legislation/HR policies. |
| Technology risks | Risks arising from technology not delivering the expected services due to inadequate or deficient system/process development and performance or inadequate resilience. |
| Information risks | Risks arising from a failure to produce robust, suitable, and appropriate data/information and to exploit data/information to its full potential. |
| Security risks | Risks arising from a failure to prevent unauthorised and/or inappropriate access to information, including cyber security and non-compliance with General Data Protection Regulation requirements. |
| Project/Programme risks | Risks that change programmes and projects are not aligned with strategic priorities and do not successfully and safely deliver requirements and intended benefits. |
| Reputational risks | Risks arising from adverse events, including ethical, a lack of sustainability, systemic or repeated failures or poor quality or a lack of innovation, leading to damages to reputation and or destruction of trust and relations. |

All high-level risks are recorded on JCAD Core (Enterprise Risk Management Software) – the Council's centrally managed real-time system to record, monitor, and report risks and mitigation actions in a structured and consistent way. JCAD software facilitates Active Risk Management and includes an audit function to track progress over time and automated email alerts to remind risk/mitigation owners to review/update their risks and actions at pre-determined times.

*Active Risk Management - Key Principles*

- Identify the risks in response to changing circumstances and in real time.
- Identify what to do about each risk.
- Decide who is responsible for the risk and mitigation actions.
- Record the details about the risk and how it will be managed changes in risk.
- Regularly monitor changes to the risk and use this learning.

Fundamentally, Active Risk Management requires all decision makers within the organisation to have a collective responsibility for managing risk but should do so proportionately and in alignment to other key management activities and priorities.

The following principles underpin the Council's risk management approach and are intended to be both practical and aspirational: practical because they inform and guide our approach to risk management; aspirational because in some cases they are objectives to work towards.

*Effective risk management should be:*

- **Embedded** integral part of decision making; aligned to governance frameworks, business planning, financial and performance management; and a significant influence on the Council's working culture.
- **Dynamic** ongoing and continuous, operating organically at different levels and across different service areas.

- **Proactive** not viewed solely as a compliance activity, but rather as a process that actively looks forward, taking account of changing circumstances and priorities to mitigate threats and explore opportunities.
- **Proportionate** focus on the things that matter, it should add value and help control potential threats.
- **Enabling** helps the Council be agile, innovative, to actively consider its risk appetite, and learn from both success and failure.
- **Owned** managed by everyone at the Council, but at the same time there needs to be clear and specific accountabilities for risk management processes, individual risks, and their associated actions.
- **Communicated** the importance the Council places on risk management is effectively communicated, and different service areas share best practice.
- **Understood** a shared understanding of the Council's approach to risk management, of the range and nature of risk it faces, and of strategies for minimising threats and maximising opportunities.
- **Robust** risk management practices are coherent, align with best practice and are supported by helpful and practical guidance.
- **Evaluated** The value of the Council's risk management approach is regularly reviewed, leading to improved approaches and practices.

*Active Risk Management Process*


Active Risk Management is a continual cycle of identifying, assessing, treating, monitoring, and reporting and should be managed alongside other key business activities such as strategic priority setting and resource planning. All high-level are routinely reviewed and considered at senior leadership team meetings so that risks remain relevant and appropriate in an ever changing social, political, and economic landscape. Local Government is a sector that constantly needs to adapt its services to meet the needs of its citizens and Active Risk Management is fundamental to achieving this.

Good risk management relies first and foremost on sound judgement and risks should be formulated using an evidence-based approach. This helps the Council focus on the right things at the right time and respond to regulatory and other statutory and compliance requirements.

Active risk management provides the Council with both structure and a standardised framework that is nationally recognised as best practice. When considering the management of risk, managers should first consider some basic questions:

- Am I actively looking to identify and manage issues that could happen, and issues that would have a detrimental impact on my service area or the wider Council?
- Am I able to assess the probability of something happening and the extent of its potential impact if it were to happen?
- Am I taking the necessary steps to address this issue/risk by taking steps to reduce its probability or constrain its likely impact?
- Am I regularly reviewing and reporting on the effectiveness and value of risk controls and mitigation actions?

*(Step 1) Identifying Risks*

The Council recognises that in identifying risk it needs to consider the full range of potential issues and activities that can impact on its ability to deliver its corporate priorities. The identification process happens both proactively and organically through discussions at senior leadership teams or during service planning activities, or reactively as part of performance monitoring. The level at which a risk is subsequently categorised and given a score is determined by the likelihood and impact of something happening in the context of delivering public services. All high-level risks are captured in one place (JCAD) to provide senior leadership teams with an integrated and holistic overview of the organisation's significant risks.

To help managers identify and assess risks the following considerations should be made:

- Clarify the scope and objectives of the issue, activity, or project and the outcomes that are being sought.
- Consider using tools such as horizon scanning, SWOT or PESTLE analysis to help understand the wider operating context.
- Consider the constraints and interdependences related to a risk.
- Consider the flow of cause and effect and any unintended consequences that might arise from pursuing the outcomes.
- Align risks to service area / directorate / corporate objectives so that at the next stage it is easier to establish their potential impact.
- Involve a range of people with different perspectives and areas of expertise
- Establish a risk register to record the risks
- Describe risks mitigating actions clearly using plain english

The following list is not prescriptive but provides some common areas/issues (in a Local Government environment) to consider when identifying, assessing, scoping, and managing potential risk:

| | |
|---|---|
| Changes in Government policy, legislation, or regulation | Stakeholder and partnership attitudes and priorities |
| Financial funding threats and opportunities | Health & Safety of citizens and staff |

| | |
|---|---|
| Future demand on limited resources | Business continuity and resilience issues arising from issues such as fire, floods, terrorism and damage to buildings and assets |
| Impact of changes to social, demographical, economic, and environmental landscape | Staff resources, morale, capacity, and wellbeing |
| Uncertainty arising from transformational changes | Unintended consequences and externalities |
| Technological change and failure | Procurement and contract management issues |
| Reputational damage | Third party and outsourced services |
| Governance and internal control arrangements | Changes in political landscape |

*(Step 2) Assessing Risks*

After a risk has been identified it then needs to be evaluated, prioritised, and measured in a controlled way that enables appropriate steps to be taken to manage and mitigate the risk. Each risk is assessed against two main dimensions; probability: the likelihood of a particular risk occurring; and impact: the estimated effect of a particular risk occurring on the delivery of services or achieving the Council's aims and objectives. Timescales should also be considered at this stage and in particular the process of mitigating the risk over time to reduce the probability or potential impact of a risk becoming reality most effectively.

Risks are assessed using a probability/impact grid (an example of which is shown below). By plotting a risk against the two different dimensions the risk owner can derive a score and associated colour coding to communicate the significance of a particular risk and to compare different risks. At this stage, the risk owner is assessing the inherent risk; that is the probability and potential impact before any actions are taken to make the risk less likely to arise and/or to mitigate its impact if it does.

| LIKELIHOOD | | | | | | |
|---|---|---|---|---|---|---|
| | Almost certain (5) | 5 | 10 | 15 | 20 | 25 |
| | Likely (4) | 4 | 8 | 12 | 16 | 20 |
| | Moderate (3) | 3 | 6 | 9 | 12 | 15 |
| | Unlikely (2) | 2 | 4 | 6 | 8 | 10 |
| | Rare (1) | 1 | 2 | 3 | 4 | 5 |
| | | Insignificant (1) | Minor (2) | Moderate (3) | Major (4) | Extreme (5) |
| | | **IMPACT** | | | | |
| **Key to colour coding:** Blue Low (1 to 4); Yellow Medium (5 to 9); Amber High (10 to 15); Red Very High (16+) | | | | | | |

A risk score is derived by multiplying the probability (Likelihood) score and the impact. Using the grid above, the possible scores therefore range from 1 (Likelihood: "rare" (1) x Impact: "insignificant" (1) = 1; to Likelihood: "almost certain" (5) x Impact: Extreme (5) = 25.

*Step 3 Risk Treatment*

Selecting the most appropriate risk treatment option(s) involves balancing the potential benefits derived in enhancing the achievement of objectives against the costs, efforts, or disadvantages of proposed actions. Justification for considering risk treatments and the operation of internal controls should be broader than solely economic considerations and should take account of wider organisational factors such as delivering sustainable public services, regulatory obligations, political commitments and the views of partner organisations and stakeholders.

Putting in place effective controls to address risk relies on good judgement and a clear understanding of the related issues and factors. There is always an obvious trade-off between the time and cost of putting in place mitigating controls and the benefit derived from reducing the probability and impact of the risk; there is no value in investing time and effort in implementing controls if there is no commensurate benefit in doing it. Even the most extensive mitigation measures may not offer the desired outcome to adequately managing every risk. Sometimes the best response is accepting or tolerating risks as part of normal business but at the same time continuing to periodically evaluate and monitor them and be prepared to respond to changing circumstances and put in place additional controls if required.

Generally, though, most risks will benefit from having controls and mitigation actions in place, but these should always be proportionate, economical, efficient, effective, timely, straightforward, and practical. The key steps when putting in place controls and mitigation actions is to:

- Determine which risks need to be controlled.
- Identify and implement controls that strike the optimum balance between cost and benefit.
- Use the probability/impact grid to assess and record both the probability and impact of the risk but also repeat this process to record a revised risk score based on consideration of the mitigation actions put in place.

Most risks are given a status of ‘treat the risk’ which will then facilitate the need to consider what mitigation actions need to be put in place to reduce the likelihood or impact of the risk. Other risks can be ‘tolerated’, meaning they are risks that the Council will accept because they are outside the Council’s immediate control or the costs of taking the necessary actions outweigh the impact of the risk happening. The following table sets out the main ways to ‘treat’ a risk:

| Risk Status | Description |
|---|---|
| Treat the risk | Treating the risk is about implementing control measures (mitigation) to manage the risk to a more acceptable level. (most risks are in this category) |
| Tolerate the risk | It can be acceptable to do nothing once a risk has been assessed, as the cost of acting may be disproportionate to the potential benefit gained. Sometimes risks are tolerated as actions cannot be implemented because they are out of the Council’s control. For example, legislative changes, external decisions etc. |
| Transfer the risk | For example, a risk is managed by transferring the financial consequences to an insurer in exchange for a premium or by transferring legal liability, in a contract, to another body which transfers some, but not all, of the risk |

| | |
|---|---|
| Terminate the risk | Circumstances change for whatever reason that mean the risk is no longer something the Council wishes to monitor or take further action on. |

*(Step 4) Monitoring & Reporting Risks*

Most of the Council's risks are recorded on the JCAD system – a standalone and fully supported software/platform available to all staff. More information about using JCAD is provided on the SCC Risk Management – Policy & Guidance page on the intranet site.

Access to JCAD needs to be authorised by the Performance & Risk Manager (paul.emeny@suffolk.gov.uk) who can also offer advice, guidance, support, and training – JCAD is a very straight forward and self-explanatory system to use, and most users only need to refer to the online resources before using the system.

Risk management should be considered as part of other business and management processes (and risk registers are generally considered alongside discussions about performance, finance, and financial resources). All high-level risks should be routinely discussed at management team meetings and actively reviewed and kept relevant. Managers should be well briefed and aware of both the progress being made and the issues that need addressing.

High-level risks are reported and reviewed by both Corporate Leadership Team and Joint Leadership Team as well as by Directorate Management Teams. In most cases, this happens on a quarterly basis, but more frequently if there is a business need to do so. The purpose of reporting risk is to:

- Provide leadership teams with a clear understanding of the current active risks have been identified and are being managed by the organisation.
- In the case of reporting corporate level risks, this is an opportunity for cross departmental challenge and oversight.
- Enable issues to be identified and appropriate action taken through the relevant Director.
- Provide accountability and transparency.

At the corporate and directorate level, risk management reporting provides information enabling each management team to have visibility of risk, including details of scoring and the mitigation actions being taken to reduce the likelihood and impact.

*Review and Moderation*

In addition to regular risk reporting, all high-level risks are reviewed annually to assess their relevance and suitability and, where appropriate, make changes in consultation with the risk owner. The annual review is an opportunity to consider the Council's risk register in its entirety - across all service areas - and consider each risk in some detail, assess the relevance, appropriateness, and whether each risk score looks in balance with others, and whether each risk has suitable mitigation actions in place and whether these are scored appropriately.

Much of the focus of the annual review is to moderate the level at which risks, and mitigation actions have been assessed, but equally to consider whether the Corporate Risk Register aligns to the Council's Business Plan and corporate priorities.

The impact of national policy decisions, external change and political context is an important consideration in ensuring new risks are identified and likewise, existing risks that are no longer relevant are considered for removal.