

# Policy Title: *Risk Management Policy*

**Summary:**

*Risk is a fact of life in an ever changing landscape. By attempting to foresee and avert problems in the delivery of services and maximise opportunities, it helps ensure that resources are used in the best way possible. Risk management is a fundamental part of how we operate and forms part of our Corporate Governance Framework.*

*This Policy and supporting Procedures are designed to support a risk culture, which is embedded in the way we work rather than having a process which itself is used to drive risk management.*

<b>Last Review Date</b>	<i>August 2024</i>
<b>Next Review Date</b>	<i>August 2025</i>
<b>Approval</b>	<i>Standards and Audit Sub Board</i>
<b>Policy Owner</b>	<i>Chief Executive</i>
<b>Policy Author</b>	<i>Chief Internal Auditor</i>
<b>Advice &amp; Guidance</b>	<i>Paul Somerset <a href="mailto:paul.somerset@gosport.gov.uk">paul.somerset@gosport.gov.uk</a></i>
<b>Location</b>	<i>Infonet</i>
<b>Related Documents</b>	
<b>Applicability</b>	<i>All GBC staff</i>

## Section One: Risk Management Statement of Policy

### 1. Statement of policy

- 1.1 The Council is committed to embedding a culture of risk awareness within everyday activities such that formal processes and unnecessary documentation can be minimised, but that risk management remains an effective part of the governance framework.
- 1.2 It is accepted that not all risks can be eliminated or mitigated and a balance must always be struck between the costs of risk reduction against the likelihood and impact of the risk (risk exposure).
- 1.3 Where the organisation is required to behave in a specific way, for example to meet legal and financial governance requirements, statutory officers have pre-determined corporate directive controls, such as the Council Constitution which have been approved by Members. Compliance with these controls should prevent governance, legal and financial threats arising in the first place. Where service controls are required these fall under the auspices of the relevant Section Head, which includes their implementation and monitoring.
- 1.4 Risk impacts can be financial loss, non-achievement of objectives, environmental damage, personal injury or ill-health, legal action and reputational damage or a mix of these. Most serious risk impacts will include financial loss, legal action **and** reputational damage but the very worst are likely to include an element of either service failure, injury or environmental damage as well.
- 1.5 Evaluation of the potential financial impact of a risk will include not only the direct costs such as fines, infrastructure repairs and liability claims but indirect costs such as loss of officer time, including support staff such as Finance and Legal, lost opportunities, increased insurance premiums and reduced funds which could impact on future service delivery.
- 1.6 The Council as a public body has to protect and preserve its ability to provide services and ensure that assets are protected against significant loss and damage and interruption to service delivery is minimised.
- 1.7 Whilst it is accepted that risk cannot be entirely eradicated, the following are areas on which the council will not compromise its position by taking a greater level of risk than is absolutely necessary and will take all reasonable steps to eliminate or mitigate the risks where identified:
  - Where there is risk of physical harm
  - Where non-compliance with legislation could lead to imprisonment or significant fines

## OBJECTIVES

<b>Our Objectives</b>
Maintain a culture of risk understanding and management throughout the Organisation
Implement a strategic approach to risk management to aid and inform the Council in making significant decisions which consider the risk profile
Determine the risk appetite of the Council when aiming to deliver its strategic objectives.
Support the Council's major projects by championing risk management throughout decision making
Ensure risk management is a key element within the Council's Corporate Governance arrangements

**SECTION TWO: Procedures****2. Roles and responsibilities**

- 2.1 It is the responsibility of all members and employees to be aware of risks when carrying out their duties and to alert the relevant service manager to any perceived threat. Managers must ensure that threats are properly evaluated and mitigated.
- 2.2 The following table details the roles and responsibilities of Members and Officers of the Council. These are not directly extracted the terms of reference of the boards but they are reflective of the purpose and nature of the boards.

Policy & Organisation Board / Standards and Audit Sub Board	<ol style="list-style-type: none"> <li>1. Monitor the effectiveness of the Council's overall risk management arrangements as part of the Governance Framework</li> <li>2. Review and approve the Council's Risk Management Policy</li> <li>3. Seek assurance that risks are being managed effectively</li> <li>4. Review the adequacy of the system of internal control as highlighted by Internal Audit</li> <li>5. Promote member compliance with the RM Policy</li> <li>6. Set the Council's risk culture and appetite</li> <li>7. Challenge the adequacy of controls or actions taken to mitigate identified risks</li> </ol>
All boards and all members	<ol style="list-style-type: none"> <li>1. Seek assurance that risks are being managed effectively</li> <li>2. Consider risk implications when making or evaluating decisions</li> </ol>
Chief Executive/ Deputy Chief Executive	<ol style="list-style-type: none"> <li>1. Determine the RM Policy and procedures and create the environment for them to work effectively including promoting and supporting a risk awareness culture,</li> <li>2. Maintain awareness and oversight of the most significant risks facing the organisation</li> </ol>

	<ol style="list-style-type: none"> <li>3. Obtain assurance from Section Heads that risks have been considered, in the delivery of their services and mitigated</li> <li>4. Challenge Section Heads on the adequacy of controls or actions taken to mitigate risks</li> <li>5. Ensure regular reporting to Standards and Audit Sub Board / Policy and Organisation Board</li> </ol>
Corporate Governance Group	<ol style="list-style-type: none"> <li>1. To seek evidence and assurance on the content of Section Risk Registers</li> <li>2. To keep under review the Risk Management &amp; Assurance Framework to ensure its adequacy &amp; effectiveness</li> <li>3. To identify any themes that arise and propose corporate actions to mitigate or escalate as appropriate</li> <li>4. To review the risk register prior to submission to Standards and Audit Sub Board / Policy and Organisation Board</li> <li>5. To ensure that assurances for key areas are mapped and any gaps in assurance addressed</li> </ol>
Section Heads / Project Managers	<ol style="list-style-type: none"> <li>1. Promote risk awareness and responsibilities to employees</li> <li>2. Consider risks to service/project delivery, via a Risk Register, and evaluate appropriate responses including the introduction and monitoring of effective control</li> <li>3. Obtain assurance that risks have been considered, in the delivery of their services and mitigated</li> <li>4. Risk assess any decisions and option analyses</li> <li>5. Report promptly to the Chief Executive/ Assistant Chief Executive any perceived new risks or significant failures in controls</li> <li>6. Maintain channels of communication to encourage bottom up reporting of risks and control failures</li> <li>7. Ensure compliance with corporate directives controls as a first response to governance financial and legal threats.</li> </ol>
Monitoring Officer/Deputy Monitoring Officer	<ol style="list-style-type: none"> <li>1. Report on significant risks to Policy and Organisation Board</li> <li>2. Maintain a Legal Risk Register of most significant risks affecting the Authority</li> <li>3. Report to Corporate Governance Group and S&amp;A/P&amp;O within the relevant timing of the risks on mitigation with either assurance or alerting to weaknesses in actions</li> </ol>
Internal Audit and Assurance	<ol style="list-style-type: none"> <li>1. Maintain the RM Policy and oversight of communications and training</li> <li>2. Carry out periodic audits on assurance and effectiveness of RM procedures</li> <li>3. Assist in providing assurance on the management of risk and effectiveness of controls</li> </ol>

Managers, supervisors, team leaders	<ol style="list-style-type: none"> <li>1. Promote risk awareness and communicate responsibilities to employees</li> <li>2. Maintain awareness of the risks within their area of responsibility</li> <li>3. Actively encourage staff to report risk concerns</li> <li>4. Evaluate risks and appropriate responses</li> <li>5. Escalate risks that have significant impact to relevant Section Heads</li> </ol>
All employees (including contractors and partners)	<ol style="list-style-type: none"> <li>1. Be aware of threats, opportunities weaknesses or failures in control in their day to day activities</li> <li>2. Comply with controls that have been set up to mitigate risks and identify where they can be strengthened</li> <li>3. Report promptly to their manager any perceived new risks, failures in controls, lost opportunities or where controls can be strengthened</li> </ol>

### 3. Training and Embedding

3.1 Embedding the risk culture will be achieved by a combination of the following:

- (1) Risk training provided to relevant Section Heads bi-annually
- (2) Risks to be considered at Section Meetings, one to ones and any other meetings held to discuss service performance, objectives, progress, new decisions, options, changes in working practices or legislation,
- (3) Risks identified by outside parties such as partners, contractors insurance providers etc. will be brought to the attention of the relevant manager and dealt with accordingly
- (4) Significant/critical risks from Audit reports will be included in the Strategic Risk Register
- (5) Significant/critical risks highlighted from Manager's responses to the governance framework will also be included in the Risk Register
- (6) The Strategic Risk Register will be reported to Corporate Governance Group regularly and based on the timing of the risks identified.

### 4. Strategic Risk Register

4.1 The Strategic Risk Register will be a formal register of all significant risks that could impact the Authority and will be maintained by the Chief Internal Auditor.

4.2 They will be recorded with the mitigating actions and person responsible.

4.3 Risks will be profiled as Significant/Critical (red) High(Amber), Medium (Yellow) or Low (Green). The levels will be determined based on the below Risk Matrix

L I K E L I H O O D	Very Likely	5	5	10	15	20	25
	Likely	4	4	8	12	16	20
	Possible	3	3	6	9	12	15
	Unlikely	2	2	4	6	8	10
	Rare	1	1	2	3	4	5
<b>Risk Rating Matrix</b>			<b>1</b>	<b>2</b>	<b>3</b>	<b>4</b>	<b>5</b>
			<b>Minimal</b>	<b>Minor</b>	<b>Moderate</b>	<b>Major</b>	<b>Critical</b>
<b>SIGNIFICANT/CRITICAL RISK</b>			<b>IMPACT</b>				
<b>HIGH RISK</b>							
<b>MEDIUM RISK</b>							
<b>LOW RISK</b>							

4.4 Each risk will contain a comment from the relevant Section Head re the risk appetite applied to the risk and any costs of mitigation. The risk will then be analysed post mitigation to determine its current profile

## 5. Risk Assessments

5.1 Significant/Critical risks will be escalated to the Strategic Risk Register by the relevant person as detailed in the following paragraphs.

5.2 Significant/Critical risks are where the threat, likelihood and impact could cause:

- The failure or unacceptable interruption of the delivery of a service that is provided to ensure support to the public
- Personal Injury or harm
- Loss of trust or integrity in the Council's dealings with others
- Ineffective use of council resources resulting in objectives not being met or reducing resources such that it impacts on the delivery of other objectives or services.
- A missed opportunity to contribute long term to objectives that would make a positive difference to how a service is delivered

5.3 Activities that will identify significant risks to be escalated to the Strategic Risk Register include but not limited to:

- Project managers/Contract leads will provide regular feedback to relevant management. Any significant risks will be escalated to the Strategic Risk Register by the Project manager/contract leads.

- Legal risks will be considered by the Borough Solicitor and Monitoring Officer and will be contained within their own register.
  - IT risks will be considered by the Head of IT and any significant risks escalated to the Strategic Risk Register by that officer.
  - Significant risks highlighted from the review of the Governance Framework will be escalated to the Strategic Risk Register by the Section Head concerned.
  - Significant risks identified by staff, DMT's, Section Heads, Partners, Contractors, Audit or inspection reports and Members must be escalated to the Strategic Risk Register by the relevant Section Head or reported to the Chief Internal Auditor for inclusion.
  - Critical Risks identified as part of any Internal Audit activity.
- 5.4 All risks will be profiled in terms of Significant/Critical, High, Medium or Low as stated in 4.3
- 5.5 Risk assessments will include direct and indirect costs of control, mitigation and exposure:
- Staff costs, including HR, Legal and Finance (support staff costs)
  - Fines
  - Legal Claims
  - Increase in Insurance premiums
  - Infrastructure repairs
  - Hidden costs such as impact on staff performance and morale
  - Reputational harm
- 5.6 Risk assessments should also include the timing of the threat e.g. is the threat likely to be in the next few months? Coming year? Winter? Summer? Etc. If a time cannot be attributed to it the threat maybe incorrectly defined.
- 5.7 Examples of areas of risk include but are not limited to:
- Business Continuity
  - Fraud
  - Security of data
  - People: Delegations, Competency of staff, compliance with Policies, Recruitment and performance, health and safety
  - Procurement and contract letting and monitoring
  - Finance; budgetary control, cash management
  - Organisation: governance, policies, priorities, consultation, communication, structures, security,
  - Service delivery; resources, partners, joint or shared working
  - Environment; buildings comply with legislation, legionella, asbestos, severe weather
- 5.8 Examples of questions to consider when assessing risks include:

- What are the threats (re fraud, business continuity etc) in particular which ones are key to your service delivery or could impact on another's service delivery?
- What are the threats that could cause a service to fail or not meet its objectives? What would the impact of that failure be?
- Are there any compensating controls and if they are robust?
- How do you gain assurance that they are?
- What is the timing of the threat? Could it happen at any time?
- What is the risk appetite? Is it ok for the threat to materialise because for example there is a backup plan that can be immediately (or quickly) implemented?
- What is the cost of the control?
- What would the cost of the threat (s) materialising be?

## **6. Assurance**

- 6.1 All Sections will have a mechanism to identify and assess risk on a continuous basis and determine mitigation. Controls introduced to mitigate threats must be monitored at regular intervals to ensure that they are effective. If they are not effective action to remedy the situation must be taken e.g. to review the control itself or enforcement. The testing of controls and any other mitigation will form the assurance that a threat is being managed.
- 6.2 Assurance must be available in the form of evidence that can be verified (e.g. business continuity business plan and testing of its robustness) where significant risks are identified. This will be tested by the Corporate Governance Group which consists of the Chief Executive, Chief Internal Auditor, Borough Solicitor, Head of Finance and the Deputy Chief Executive.

## **7. Monitoring and Review**

- 7.1 The Strategic Risk Register will be considered by the Corporate Governance Group in accordance with timings of risks. The Strategic Risk Register will be presented to the board biannually however should a significant risk arise without an ability to manage the risk, the Chair of the Board will be notified with the option to convene an extraordinary meeting if deemed required.
- 7.2 Managers are responsible for monitoring their own risks in accordance with this policy and procedures and escalating where relevant.