Policy Title: *Risk & Assurance Management*

Portsmouth CITY COUNCIL

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.

These Policy and 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.

ID	*RM-002*
Last Review Date	*June 2018*
Next Review Date	*June 2020*
Approval	*G&A&S*
Policy Owner	*Director of HR, Legal and Performance*
Policy Author	*Corporate Performance Manager*
Advice & Guidance	*Kelly Nash 023 9268 8157 kelly.nash@portsmouthcc.gov.uk*
Location	*Policy hub*
Related Documents	http://intralink/Media/HST_2012_Apr_Corp_Health_and_Safety_Pol_3rd_edition.pdf
Applicability	*All PCC staff*

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 to meet legal and financial governance requirements for example, statutory officers have determined corporate directive controls, such as the City 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 head of service, 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, loss of staff morale and productivity, 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

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 the 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

Governance and Audit and Standards Committee	1. Monitor the effectiveness of the Council's overall risk management arrangements as part of the Governance Framework 2. Review and approve the Council's Risk Management Policy 3. Seek assurance that risks are being managed effectively 4. Review the adequacy of the system of internal control as highlighted by Internal Audit 5. Promote member compliance with the RM Policy
Cabinet/ Portfolio Holders/ all Members	1. Seek assurance that risks are being managed effectively 2. Set the Council's risk culture and appetite 3. Consider risk implications when making or evaluating decisions 4. Challenge the adequacy of controls or actions taken to mitigate identified risks.
Chief Executive/ Deputy Chief Executive	1. Determine the RM Policy and procedures and create the environment for them to work effectively including promoting and supporting a risk awareness culture, 2. Maintain awareness and oversight of the most significant risks facing the organisation 3. Obtain assurance from Directors that risks have been considered, in the delivery of their services and mitigated 4. Challenge Directors on the adequacy of controls or actions taken to mitigate risks 5. Ensure regular reporting to Governance and Audit and Standards Committee
Corporate Governance Group	1. To keep under review the Risk Management & Assurance Framework to ensure its adequacy & effectiveness 2. To identify any themes that arise and propose corporate actions to mitigate or escalate as appropriate 3. To review the risk register prior to submission to

	Governance and Audit and Standards Committee 4. To ensure that assurance for key areas is mapped and any gaps in assurance addressed
Directors	1. Promote risk awareness and responsibilities to employees 2. Consider risks to service delivery and evaluate appropriate responses including the introduction and monitoring of effective control 3. Obtain assurance that risks have been considered, in the delivery of their services and mitigated 4. Risk assess any decisions and option analyses 5. Report promptly to the Chief Executive/ Deputy Chief Executive & relevant Portfolio Holders any perceived new risks or significant failures in controls 6. Maintain channels of communication to encourage bottom up reporting of risks and control failures 7. Ensure compliance with corporate directives controls as a first response to governance financial and legal threats. 8. Where Directors are acting as Project Directors they must ensure that risks have been considered and mitigated (where possible) recorded and form part of the information to the Corporate Governance Group and Members
Strategy Unit	1. Maintain the RM Policy and oversight of communications and training 2. Report on significant risks to G&A&S 3. Maintain a Directory of most significant risks affecting the Authority 4. Report to Corporate Governance Group and G&A&S within the relevant timing of the risks on mitigation with either assurance or alerting to weaknesses in actions
Internal Audit and Assurance	1. Carry out periodic audits on assurance and effectiveness of RM procedures 2. Assist in providing assurance on the management of risk and effectiveness of controls
Managers, supervisors, team leaders	1. Promote risk awareness and communicate responsibilities to employees 2. Maintain awareness of the risks within their area of responsibility 3. Actively encourage staff to report risk concerns 4. Evaluate risks and appropriate responses 5. Escalate risks that have significant impact to relevant Directors

All employees (including contractors and partners)	1. Be aware of threats, opportunities weaknesses or failures in control in their day to day activities 2. Comply with controls that have been set up to mitigate risks and identify where they can be strengthened 3. Report promptly to their manager any perceived new risks, failures in controls, lost opportunities or where controls can be strengthened

3. Training and Embedding

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

(1) E-learning on Risk Awareness to be completed as part of induction and every three years thereafter by all staff
(2) Risk alert forms to be available on Intralink for staff to report risks to their manager
(3) Risks to be considered at DMT's, meetings with portfolio holders, one to ones and any other meetings held to discuss service performance, objectives, progress, new decisions, options, changes in working practices or legislation,
(4) 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
(5) Significant risks from Audit reports will be included in the Risk & Assurance Directory
(6) Significant risks highlighted from Managers responses to the governance framework will also be included in the Risk & Assurance Directory
(7) The Risk & Assurance Directory will be reported to Corporate Governance Group based on the timing of the risk.

4. Risk and Assurance Directory

4.1 The Risk & Assurance Directory will be a formal register of all significant risks that could impact the Authority and will be maintained by the Strategy Unit.

4.2 They will be recorded in assurance categories (see 6.3) with the mitigating actions and person responsible.

4.3 Risks will be profiled as High (red) Medium (Amber) or Low (Green).

4.4 Each risk will contain a comment from the relevant Director re the risk appetite applied to the risk and any costs of mitigation.

5. Risk Assessments

5.1 Significant risks will be escalated to the Risk & Assurance Directory by the relevant person as detailed in the following paragraphs.

5.2 Significant 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 vulnerable people, or to protect the environment
- 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 Risk & Assurance Directory include:

- Project managers will provide regular feedback to relevant project boards. Any significant risks will be escalated to the Risk & Assurance Directory by the Project Director either directly to the Chief Executive/ deputy Chief Executive or via performance returns dependent on timing of the risk

- Legal risks will be considered by the Deputy Chief Executive and Resources Portfolio holder and will be contained within their own register .

- IT project risks will provide regular feedback to the project board/sponsor and any significant risks escalated to the Risk & Assurance Directory by the Project Manager.

- Significant risks highlighted from the review of the Governance Framework will be escalated to the Risk & Assurance Directory by the Director concerned.

- Significant risks identified by staff, DMT's, Directors, Partners, Contractors, Audit or inspection reports and Members must be escalated to the Risk & Assurance Directory by the relevant Director or reported to the Corporate Performance Manager for inclusion.

5.4 All risks will be profiled in terms of High Medium or Low as stated in 4.2.

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:

- 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? What would the impact of that failure be?
- Are there are 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 Directorates 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. This 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.

6.3 To give assurance on the key areas (as defined from time to time by the Corporate Governance Group) an assurance map showing the evidence to support the management of those areas will be compiled and maintained by the Internal Audit Service. This map will currently cover the following areas:

- Financial risks including risk of/exposure to fraud
- Technical eg. cybercrime, system failure and disaster recovery
- Political including decision-making
- Legal risk, including fulfilling Statutory obligations
- Specific vulnerabilities including Legionella, Data Protection, Fire risk etc

7. Monitoring and Review

7.1 The Risk & Assurance Directory and assurance map will be considered by Corporate Governance Group and G&A&S in accordance with timings of risks.

7.2 Managers are responsible for monitoring their own risks in accordance with this policy and procedures and escalating where relevant