Ombwdsmon Ombudsman
OMBWDSMON GWASANAETHAU CYHOEDDUS CYMRU
PUBLIC SERVICES OMBUDSMAN FOR WALES

Risk Management Policy

Mae'r ddogfen hon hefyd ar gael yn y Gymraeg
This document is also available in Welsh

Risk Management Policy

Contents

Risk Management Policy

1 Risk Management - Introduction

1.1 **Risk** is defined as being the threat that an event or action will adversely affect the organisation's ability to achieve its objectives and to successfully execute its mission.

1.2 **Risk Management** is defined as the process by which risks are identified, evaluated and controlled.

1.3 PSOW recognises it has a responsibility to manage both internal and external risks as a key component of good corporate governance. It is committed to embedding risk management into the daily operations of the organisation from the setting of objectives, to service and financial planning through to departmental processes. It believes that effective risk management will help it to achieve its corporate objectives.

2 Aims

2.1 The organisation's approach to risk management aims to:

- Integrate risk management into the culture of the organisation (policy planning, operational management and individual employees' roles);
- Manage risk in accordance with best practice, taking action to minimise the likelihood of risks occurring and /or reduce the severity of consequences should risks occur;
- Anticipate and respond to social, environmental and legislative requirements;
- Prevent injury, damage and losses and reduce the cost of risk;
- Raise awareness of the need for risk management;
- Identify, eliminate or minimise the risks of fraud;
- Ensure that risks are monitored on an ongoing basis, discussed at Management Team quarterly, and reported to the Audit & Risk Assurance Committee as required.

3 Process

3.1 The organisation will adopt the following process to identify and manage

risks.

- The risk report owner is to ensure the current risk report is accessible by all PSOW staff
- Any staff can identify additional risks, and all staff are encouraged to identify and escalate risks as they are identified and at team meetings
- Once a risk has been identified the member of staff must inform their Line Manager.The Line Manager is to inform the risk report owner via the minuted team meeting minutes, or for urgent matters direct with Risk Report Owner (or Chief Operating Officer in the absence of the risk report owner).
- Risk must be a standing agenda item for all team meetings and any risks identified at team meetings must be minuted.
- The risk report owner is to report to Management Team the up to date position with proposals for additions / deletions and amendments.

3.2 Management Team will discuss and agree, for each risk in the risk report:

- Identified (inherent/current) risk
- Likelihood and impact
- Risk rating
- Whether to accept, manage, reduce or eliminate
- Controls and mitigating actions (in place or additional)
- Residual risk
- Assurance method

3.3 Management Team will approve the risk report, amended or updated as appropriate.

3.4 The risk report owner will publish the updated risk report which will be available to all staff.

4 Reporting to Audit and Risk Assurance Committee

4.1 The Risk Management report is to be considered by the Audit & Risk Assurance Committee on a quarterly basis.

5 Roles and Responsibilities

5.1 The Audit & Risk Assurance Committee

- Oversee the effective management of risk by Management Team.
- Review identified risks and actions as reported by Management Team and consider whether there appear to any additional significant risks or additional mitigation measures or additional sources of assurance.

5.2 Management Team

- Take a lead in identifying and managing the strategic risks and opportunities facing the organisation.
- To escalate risk issues raised by staff, individually or at team meetings.
- To consider the strategic and key operational risks.
- To develop and implement a comprehensive and structured approach to risk management.
- To determine the organisation's risk appetite and priorities for action.
- To ensure that risk management is part of the decision-making process and to provide appropriate challenge.
- To provide an assurance to Audit & Risk Assurance Committee that effective risk management is being implemented.

5.3 Line Managers

- To ensure risk is considered at all times during team meetings
- To have a standing agenda item on all team meetings for 'risks identified during meeting discussions

- To report to risk report owner any identified risks either arising from team meetings or any others identified outside of meetings.

5.4 Risk Report Owner (IT Manager)

- To manage and monitor the risk report;
- To report to Management Team on risk management;
- To report to the Audit & Risk Assurance Committee on risk management;
- To collate identified risks and propose changes / additions / deletion;
- To ensure risk is considered at Management Team meetings for all items discussed; and
- To liaise with individual teams at regular intervals to promote and discuss risks, promoting greater awareness of risk within the organisation.

5.5 All Staff

- Individual members of staff to manage risk effectively in their jobs;
- Individual members of staff to be responsible for identifying risks in their areas and, where appropriate, proposing mitigating actions;
- Individual staff to report to risk report owner (or via line manager) any identified risks.

6 Risk Appetite

6.1 Definition

6.1.1 Risk is inherent in the provision of all public services. In view of the role of PSOW in promoting good practice and good governance by public bodies, it is important that its own processes comply to the standards to which bodies under jurisdiction are expected to adhere. The Office must also ensure that its reputation and integrity is such that members of the public have confidence in raising complaints, and that its decisions are soundly based.

6.1.2 The Ombudsman's approach to risk is that risks will be identified, assessed

and managed, with appropriate action taken to mitigate or eliminate risks where possible. In managing risks, the Ombudsman will take account of the potential benefits as well as the likelihood and scale of risks.

6.1.3 Innovation and engagement in improving public services requires risk taking. The Ombudsman and his staff will seek to manage risk well.

6.1.4 The Ombudsman recognises that it is not appropriate to have a single view of all risks, but rather to assess the appetite for risk for particular risks and aspects of its activities. These are considered further in 6.5 below.

6.2 Risk horizons

6.2.1 Identification & Assessment of Risk will be based upon a number of key areas or 'Risk Horizons'. Staff, team meetings, Management Team and Audit & Risk Assurance Committee will consider risks against each horizon and highlight new or increasing risks. The key risks and planned actions can be considered and reviewed.

6.2.2 The Risk Report Owner (IT Manager) will draw risk horizon information from staff members, team meetings, Management Team or Audit & Risk Assurance Committee, collate them and update the risk report. This report will then be presented to Management Team and Audit & Risk Assurance Committee quarterly. The format is intended to encourage focussed discussion and detailed consideration of the greatest risks and associated mitigation or remedial actions.

6.2.3 The key risk horizons are:

- Operations, including operational support
- Financial
- Reputational
- Governance and Legal
- Data & Information Management

6.2.4 All risks identified under each horizon will be included in the quarterly risk management report to Management Team and Audit & Risk Assurance

Committee. For each horizon ongoing and one-off risks will be identified and considered.

6.2.5 **Operations** includes staffing levels & skills, adequacy of systems & processes, resources, caseload & throughput, support processes, support staff, facilities, telephony and ITC systems.

6.2.6 **Financial** risk includes adequacy of financial resources, budgets, financial processes and systems, financial monitoring, accounting and audit issues and risks arising from (expected and unexpected) financial pressures.

6.2.7 **Reputational** risk includes risks relating to public, relevant body, scrutiny body or media reactions to our actions or decisions.

6.2.8 **Governance and Legal** risks include reporting, accountability, Advisory Panel and Audit & Risk Assurance Committee, audit arrangements, compliance with legal requirements and strategic & operational planning.

6.2.9 **Data & Information Management** includes data security incidents, any matters considered by the Information Commissioner's Office, physical and cyber information security and compliance with Data Protection and Information Security regulations.

6.2.10 It is acknowledged that some risks, such as the risk of fraud and corruption, could affect more than one of these risk horizons. Such risks will be considered in the most appropriate risk horizon, taking account of the control measures (for example financial systems / processes or governance / accountability).

6.3 Risk status

6.3.1 The risk status will be shown for the **current** position taking account of controls and mitigation already in place ('**inherent risk**') and for the risk expected to remain after specified **additional** mitigation and control measures are put in place ('**residual risk**'). Risk status for each will be shown as follows:

- **Red:** Any serious risk where urgent attention and action may be required

- **Amber:** New risk or risk that requires particular attention
- **Green:** Ongoing lower level risk

6.3.2 The Risk Report Owner (IT Manager) will draw risk status information from staff members, team meetings, Management Team or Audit & Risk Assurance Committee, collate them and update the risk report and risk register to be included in the quarterly report to Management Team and Audit & Risk Assurance Committee

6.4 Categories of risk appetite

6.4.1 The risk appetite of any organisation and any area of risk can be described as one of the following:

- **Averse:** The avoidance of risk and uncertainty is a key organisational objective.
- **Minimal:** Has preference for ultra-safe business delivery options that have a low degree of inherent risk and have a potential for only limited reward.
- **Cautious:** A preference for safe delivery options that have a low degree of inherent risk and may have only a limited potential for reward
- **Open:** A willingness to consider all potential delivery options and choose the one that is most likely to result in successful delivery while also providing an acceptable level of reward and value for money.
- **Eager:** Has an eagerness to be innovative and to choose options offering potential higher business rewards (despite greater inherent risk).

6.5 Assessment of PSOW risk appetite

6.5.1 Applying the categories of risk appetite above, the PSOW risk appetite, for the different aspects of its activities, is as follows:

- **Operations & operational support - Casework decisions, investigations and findings:**

Cautious - The organisation recognises the fundamental importance of maintaining the confidence of the public, providers of public services and others including the media and politicians in the quality of its investigations and robustness of its decisions and findings.

- **Governance, Financial - Reputation and public perception:**
  Open - The organisation is clear that it must operate to the highest standards of probity but is open to innovation, value for money and the early adoption of best practice.
- **Governance:**
  Cautious - It is essential that the organisation can demonstrate that it has robust and appropriate governance arrangements and follows best practice.
- **Governance - Compliance with legal and financial requirements:**
  Minimal - The organisation must ensure that it complies fully with statutory requirements.
- **Data Privacy / Information Security:**
  Averse – Minimal - Safeguarding of confidential information is paramount.
- **Core function - Public profile and measures to improve public services:**
  Open – Eager - The organisation understands that to prompt necessary improvement in public service providers it can be necessary to be outspoken and clear. This creates a risk of adverse reaction from the public service providers involved, politicians or the media. The organisation will not act without clear concerns evidenced by casework but recognises that this may prompt challenges to the Ombudsman and public criticism. The organisation also accepts that some complainants will be unhappy that their complaints are not upheld and may seek to discredit the organisation. This will not deflect the organisation from making appropriate decisions on casework.
- **Core function, Operational support - New approaches to service delivery, procurement and communication:**
  Open - Eager - The organisation is open to innovation, working in different ways and increasing its profile, and accepts that some approaches that it tries may be unsuccessful. The requirements above

in terms of casework decisions and probity do, however, remain paramount.

7 Review and publication

7.1. This policy will be reviewed annually and will be published internally and externally.

7.2. Any questions about this policy can be directed to policycontrol@ombudsman.wales.