Ombwdsmon
Ombudsman
Cymru • Wales

Risk Management Policy

Mae'r ddogfen hon hefyd ar gael yn y Gymraeg.

This document is also available in Welsh.

Content

1. **Risk Management - Introduction** 3
2. **Aims** 3
3. **Process** 4
4. **Reporting to Audit and Risk Assurance Committee** 6
5. **Roles and Responsibilities** 7
6. **Risk Appetite** 9
7. **Review and publication** 15

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 An **issue** is a risk that has materialised. Issues will be managed to ensure steps are taken so they do not impact on the organisation's ability to achieve its strategic objectives.

1.4 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 operational processes. It believes that effective risk management will help it to achieve its corporate objectives. Similarly, early identification of issues, as defined above, will help the organisation to minimise their impact and duration. This policy includes the management of issues as well as risks.

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 including monthly team meetings 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.

2.2 The organisation's approach to managing **issues** is that they are recorded on the Risk and Issues Register once the risk has materialised, with appropriate actions that are discussed at Management Team quarterly and reported to the Audit & Risk Assurance Committee.

3. Process

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

- The risk report owner is to ensure the current risk and issues 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 Once a risk has developed into an issue it will be highlighted as such on the Risk and Issues Register, with appropriate actions that will reduce the impact of the issue and/or its duration, with a view to minimising its impact on the achievement of organisational objectives.

3.3 Management Team will discuss and agree, for each risk and issue in the risk and issues report:

- Identified (inherent/current) risk
- Likelihood, impact and direction of travel
- Risk rating
- Whether to tolerate, treat, transfer or terminate the risk
- Any risks that have become issues (or any issues arising without a corresponding identified risk)
- Controls and mitigating actions (in place or additional), together with assigned responsibilities and timescales
- Residual and target risk
- Assurance method

3.4 Risks are scored based on the impact and likelihood based on the scoring matrix detailed in the Risk and Issues Register, using the ratings below:

Likelihood:		
1	Extremely unlikely	Rare / may occur in exceptional circumstances
2	Unlikely	Could occur at some time
3	Possible	Might occur at some time
4	Probable	Likely to occur at some time
5	Very likely	Almost certain / is expected to occur
Impact:		
1	Minor	e.g. 1 day disruption
2	Not significant	e.g. 2+ days disruption
3	Significant	e.g. 3+ days disruption
4	Serious	e.g. > 5 days disruption,
5	Major	e.g. > 10 days disruption

Impact ratings can take into account financial impact, disruption to service, reputational impact / loss of confidence, legal/regulatory risk and impact on staff/staffing. This list is illustrative, and any impact can be included.

3.5 The register will show a current risk score, which is an assessment of where we are now, and a target risk score based on the risk appetite, which will be the score we aim to reach once we have implemented all actions and controls.

3.6 The Risk and Issues Register will show where the assurance has been gained from, and this will be through one of the 4 lines of defence. The 4 lines of defence refer to different layers of protection to manage and mitigate risks effectively. They are:

- First line: Operational teams and individuals directly responsible for the day-to-day activities.
- Second line: Risk management and compliance functions that provide oversight and guidance.
- Third line: Objective and independent assurance, such as the Audit & Risk Assurance Committee and Internal audit, who provide an independent evaluation of the effectiveness of internal controls.
- Fourth line: External audit and other regulatory bodies, who ensure compliance with relevant laws and legislation.

3.7 Management Team will approve the risk and issues report, amended or updated as appropriate.

3.8 The risk report owner will publish the updated risk and issues 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

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.

Management Team

- Take a lead in identifying and managing the strategic risks and opportunities facing the organisation.
- 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.
- Annually to review and challenge the risks on the Risk and Issues Register so that the Register remains relevant and fit for purpose.
- To provide an assurance to Audit & Risk Assurance Committee that effective risk management is being implemented.

Line Managers

- To ensure risk is considered during team meetings.
- To have a standing agenda item on all team meetings for risks identified.
- To report to risk report owner any identified risks either arising from team meetings or any others identified outside of meetings.

Risk Report Owner (Finance Manager)

- To manage and monitor the risk report.
- To collate and escalate to Management Team, as appropriate, any risk issues raised by staff, individually or at team meetings.
- To collate risks shared with the organisation through internal/external audit briefing notes, and from other sources such as external training events, once an assessment has been made as to whether they are relevant to PSOW.
- To report to Management Team on risk management.
- To report to the Audit & Risk Assurance Committee on risk management.
- To collate identified risks and issues, and to propose changes / additions / deletion.
- To ensure risk is considered at Management Team meetings for all items discussed.
- To liaise with individual teams at regular intervals to promote and discuss risks, promoting greater awareness of risk within the organisation.

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

Definition

6.1 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.

6.2 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.

6.3 Innovation and engagement in improving public services requires risk taking. Innovation and measures to manage our increasing workload similarly may result in activities with different levels of risk. The Ombudsman and her staff will seek to understand and manage risk well.

6.4 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 6.21 below.

6.5 The organisation is aware that there are risks associated with not taking action and not embracing change, as well as risks of taking action. The risk of not doing something is considered and addressed as part of normal business.

Risk horizons

6.6 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.

6.7 The Risk Report Owner (Finance Manager) will draw risk horizon information from staff members, team meetings, Management Team or Audit & Risk Assurance Committee, collate them and update the risk and issues register. 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.

6.8 The key risk themes are:

- Casework
- Staffing
- Technology
- Financial
- Reputational
- Governance and Legal
- Data & Information Management

6.9 All risks identified under each theme 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.

6.10 **Casework** risk includes our approach to all our casework decisions, including our processes, decision making and adequacy of findings. It also includes the ongoing implementation of our proactive powers.

6.11 **Staffing** risk includes the skills and diversity of our workforce, our staff resources across teams, the health and safety, wellbeing and attendance of staff and our approach to segregation of duties and succession planning.

6.12 **Technology** risk includes the adequacy of our ITC and telephony systems, our approach to cyber security and cloud services, resources to support hybrid working and our incident management responses.

6.13 **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.

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

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

6.16 **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.

6.17 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).

Risk status

6.18 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

6.19 The Risk Report Owner (Finance 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 and issues register to be included in the quarterly report to Management Team and Audit & Risk Assurance Committee

Categories of risk appetite

6.20 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).

Assessment of PSOW risk appetite

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

- **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.

- **Casework – Approach to public service improvement:**

  Open – There is an opportunity for us through our ongoing work on complaints standards to drive a fundamental change in public services. To do this we will have to work with public bodies to bring about change in their own organisations. Furthermore, we can be ambitious in our use and choice of Own Initiative investigations to target the areas where the greatest impact and change can be achieved. As with all casework decisions, our approach to any Own Initiative investigation decision will remain sound and unaffected by this higher level of risk.

- **Casework – Internal processes and approach to technology:**

  Open - Eager – We are facing continued increases in the volume and complexity of cases, therefore there is a need to do things differently and embrace new approaches to service delivery. This includes changes to our internal processes to improve throughput of cases and achieve greater efficiency, and in the use of new technology, such as chatbots or Artificial Intelligence, to reduce human input in basic tasks to free up time to deal with casework. We accept that some of these approaches may be unsuccessful and that our approach to casework decisions and probity remain sound and unaffected.

- **Staffing – Attendance and wellbeing:**

  Averse – It is key that we have the right people in the right place at the right time with the right skills. We need to avoid actions that place unnecessary negative impacts on the wellbeing of our staff so that they continue to feel valued and achieve their best.

- **Staffing – Resources:**

  Cautious – The organisation can be ambitious in our approach to recruitment to ensure that we are hiring the right type of people that best fill the role that we need. We must also manage our staff resources so that they are diverted to the areas of our work where the most attention is needed, for example switching staff from Assessment to Investigation Teams.

- **Technology – Quality of systems, hardware and software:**

  Cautious – The organisation must ensure that our internal systems remain fit for purpose to allow staff to carry out their day-to-day jobs. This means we must take a safe delivery option to technology replacement so that there is minimal impact on staff, and on the cyber security of our systems.

- **Technology – Cyber security:**

  Minimal – Given the risks associated with cyber security threats, and the significant effects a cyber incident can have, it is important to operate in a secure and safe way. As there is considerable reliance on third-party providers and cloud-hosting, management of some technology risks will be through supply chain management.

- **Financial - Reputation and public perception:**

  Cautious - The organisation is clear that it must operate to the highest standards of probity but is open to innovation, value for money and using our limited resources in a way which achieve the maximum benefit to the organisation.

- **Financial – Adequacy of future resources:**

  Open – It is important that the organisation is ambitious in seeking the resources needed to deliver its functions with impact. All funding options should be considered, and the level of resources sought should reflect need as well as taking account of the financial climate and the approaches of other directly funded bodies.

- **Governance and Legal:**

  Minimal - The organisation must ensure that it complies fully with statutory requirements. It is essential that the organisation can demonstrate that it has robust and appropriate governance arrangements and follows good practice.

- **Data & Information Management:**

  Averse – Minimal - Safeguarding of confidential information is paramount.

- **Reputation - 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.

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.