General Pharmaceutical Council

# GPhC Risk Management Policy and Guidance

## Contents

## Risk Management Policy Statement

Everything that we do as an organisation involves a degree of risk whether it is innovative projects, purchasing new systems and equipment, determining priorities, or taking decisions about the future of pharmacy regulation. It is therefore an essential part of good governance that we manage these risks effectively.

Effective risk management helps us to:

- Successfully achieve corporate priorities and objectives by capitalising on opportunities and minimising threats;
- Strengthen corporate governance and internal control framework;
- Improve partnership arrangements;
- Embed risk management into corporate processes including the financial and strategic planning.

The updated Risk Management Policy explains how GPhC will manage risk. Council and the Executive are committed to embedding the principles and practices of risk management in the culture, behaviours, processes and administration of the organisation.

David Prince
Chair of Audit & Risk Committee

Duncan Rudkin
Chief Executive & Registrar

## Risk Management Guidance

### 1. Introduction

1.1 The delivery of an organisation's objectives is surrounded by uncertainty which poses threats to success. ISO 31000:2009 Risk Management – Principles & Guidelines defines risk as 'the effect of uncertainty on objectives'.

1.2 A risk is an event, which if it occurs, could adversely impact the work of the GPhC. It may be a one-off event, repeated events or a progressive continuum.

1.3 The Standard also defines Risk Management as 'the culture, policies and processes directed towards realising opportunities whilst managing threats'. Its purpose is not to eliminate risk, but to understand it so as to take advantage of the upside and minimise the downside

1.4 GPhC's internal control systems include embedded arrangements for identifying, assessing and managing risks. Risk management is also closely linked to the business planning process.

### 2. Purpose of the Policy

2.1 The aim of this document is to create:

- A risk management framework;
- Develop a strategic risk management approach to the principal risk facing the organisation; and
- Introduce appropriate processes to assist managers in the identification and management of risk in their areas of responsibility

2.2 The key objectives of this guide are to introduce appropriate processes to:

- Develop a robust approach to identification and understanding of risks facing the organisation
- Establish practices and procedures to mitigate risk and maximise opportunities.
- Identify resources required to identify, manage, control and evaluate risks

### 3. Accountabilities, Responsibilities & Organisational Framework

3.1 The **Council** is accountable and responsible for ensuring that the GPhC has an effective programme for managing all types of risk.

3.2 The **Audit & Risk Committee** ensures that an effective system of internal control for risk management is maintained. It meets four times a year and reports directly to the Council. The Committee will agree an annual audit plan with reference to the identified strategic risks. Copies of papers for Audit & Risk Committee meetings are available to view on the intranet on the Governance Team page.

3.3 The **Chief Executive** is responsible for risk management within the GPhC and reports on it to the Council via a regular risk management review.

3.4 The **Executive Team** works with the Chief Executive to identify risks and ensure that they are properly managed.

3.5 **Managers** and **teams** are responsible for the identification of risks within their area and for escalating risks to directorate risk registers as appropriate.

3.6 *Appendix A* shows the organisational structure for risk management and assurance.

3.7 **Risk Registers**

3.7.1 The achievement of GPhC's strategic plan and objectives will carry a number of risks. The risks that could prevent the organisation from achieving its objectives are described as principal risks and are recorded in the strategic risk register.

3.7.2 Principal risks are those risks which can have organisational-wide impacts and are cross cutting or strategic in nature.

3.7.3 Risks that could impact the work of the GPhC but would not have a strategic impact are described as operational risks and a recorded in the directorate risk registers, and the team and project risk registers that sit beneath them.

3.7.4 To facilitate the management of risk throughout the organisation, the GPhC maintains a system of risk registers.

- The **Strategic Risk Register (SRR)** records the principal risks facing the organisation; those risks that could prevent the organisation from achieving its strategic plan and objectives. The risks on the SRR are identified through the Executive's assessment of the risks to the organisation's Strategic Plan. This exercise is reviewed by both Council and the Audit and Risk Committee. Operational risks that have been identified and are considered to have a strategic impact should they be realised are also recorded on the SRR. The SRR is maintained by the Head of Governance on behalf of the Chief Executive and is presented in its entirety to the Audit & Risk Committee at every meeting. The Council receives the SRR four times a year. Appendix B describes the annual risk management cycle for the Executive, Audit and Risk Committee and Council.
- **Directorate Risk Registers** provide a record of the operational risks facing each directorate. Each director takes responsibility for risks in their own area of work. All

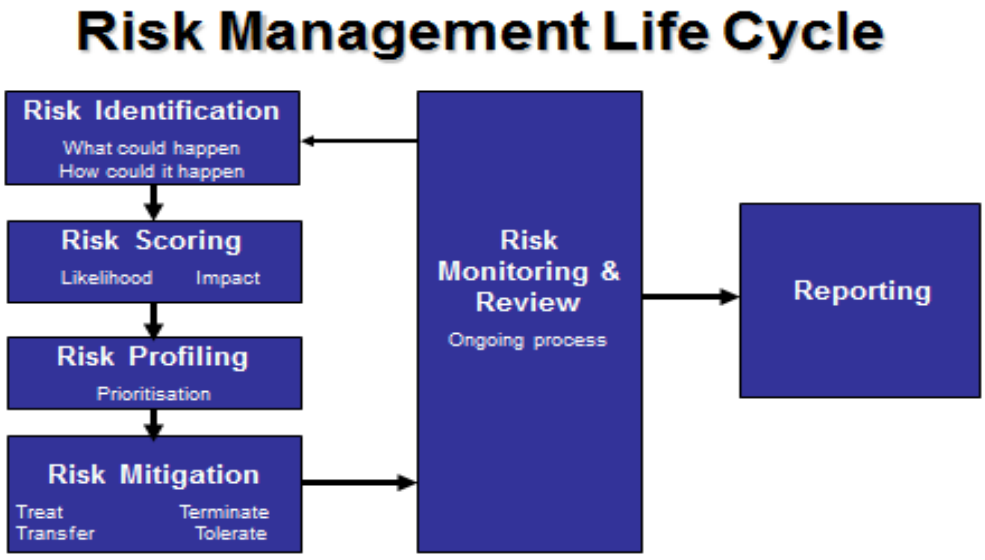
identified risks should be recorded in their directorate risk register, which should be reviewed and updated regularly. Directorate risk registers are an amalgamation of the team risk registers within the directorate. Each head of function is responsible for ensuring that the risks to the department's work and objectives are recorded and managed. The director and directorate management team may identify risks that span the directorate and these would be recorded in the directorate risk register.

- **Project Risk Registers** provide a record of the risks that have been identified from individual projects. Project risks are escalated to the either directorate risk registers via the relevant director or to the SRR via the Executive. There are three criteria for the escalation of project risks; high risk score, exceeding project tolerance levels and dependencies between projects. Project leads are responsible for maintaining the project risk registers. The Risk and Assurance Manager will assist projects with the moderation and escalation of risks as appropriate.

3.7.5 *Appendix C* provides an overview of how risks are escalated to the strategic risk register.

## 4. Risk Management Life Cycle

4.1 The process of managing risk in the GPhC ensures that risk registers at all levels remain live documents. The life Cycle has the following key elements:



## 4.2 Risk Identification

4.2.1 In order to manage risk, the organisation needs to know what risks it faces and be able to evaluate them. Identifying risks is the first step in building the organisation's risk profile. Care should be taken to avoid identifying risks that do not impact on the organisations aims and objectives.

4.2.2 The tables below details a method commonly used to identify risks in both the external and internal environment. Other methodologies which can also be used include:

- Strengths, Weaknesses, Opportunities & Threats (SWOT)
- Brainstorming
- Challenge Sessions
- Team discussions

| Pestle Analysis | | |
|---|---|---|
| **Type** | **Risk Definition** | **Examples** |
| **P**olitical | Changes in Government policy. | • Inappropriate strategic priorities<br>• Poor horizon scanning.<br>• Inability to modernise/innovate. |
| **E**conomic | Ability to meet Council's financial commitments. | • Missed business opportunities<br>• Material misuse of resources or fraud<br>• Increased cost of capital |
| **S**ocial | Social factors affecting the ability of the Council to deliver strategic objectives. | • Demographic change<br>• Crime and disorder<br>• Shortage of trained staff.<br>• Capability & capacity issues |
| **T**echnological | Failure to keep pace with technological change. | • Obsolescence<br>• Increase downtime<br>• Major IT or project failure |
| **L**egislative and Regulatory | Ability to manage current changes in UK and/or EU law/regulation | • Significant breaches of statutory legislation.<br>• Failure to follow internal policies and procedures.<br>• Inadequate response to legislative changes |
| **E**nvironmental | Environmental consequences of strategic objectives | • Noise, contamination, pollution<br>• Environmental Footprint<br>• Disposal of unused Medicines |
| Customer | Ability to meet changing customer needs and expectations. | • Poor stakeholder management<br>• Dissatisfied customers<br>• Poor Image |

## 4.3 Risk Definition & Description

4.3.1 The definition of the principal risks and uncertainties should be sufficiently specific that stakeholders can understand why they are important to the organisation. The risk

should be further described in relation to its likelihood of occurrence and the possible impact and consequences on the organisation.

### 4.4 Risk Ownership

4.4.1 Risks should be identified at a level where a specific impact can be identified and a specific action or actions to mitigate the risk can be identified. All risks, once identified, should be assigned to an owner who has responsibility for ensuring that the risk is managed and monitored over time. A risk owner, in line with their accountability for managing the risk, should have sufficient authority to ensure that the risk is effectively managed. The risk owner need not be the person who actually takes the action to address the risk. Risk owners should however ensure that the risk is escalated where necessary to the appropriate level of management. All risks on the SRR must be assigned to a member of the executive team as the owner.

### 4.5 Risk Assessment

4.5.1 Risk assessment is concerned with the measurement of identified risk. Risk is measured on two distinct scales: -

- The likelihood or frequency of the risk event occurring (on a 1 to 5 scale), and
- The severity or impact of that risk event occurring (on a 1 to 5 scale).

4.5.2 The scores for each are then multiplied together to give a risk rating (on a 1 to 25 scale) which will ultimately form the basis for allocating resources to implementing risk control and mitigation activity.

4.5.3 Risk assessment and risk scores should be graded in line with the risk matrix & risk evaluation guide as shown at Appendix D.

4.5.4 Once risks have been assessed, the risk priorities for the organisation will emerge. The greater the exposure to risk, the higher the priority assigned to addressing it. The highest priority risks (the extreme risks and those with the potential to have a strategic impact) should be given regular attention at the highest level of the organisation.

### 4.6 Risk Mitigation and Management

4.6.1 Where the risk assessment and profiling process has identified potential risk exposures, internal controls that are currently in place should be identified, along with the assurance on those controls:

4.6.2 Controls are identified as those which are:

- In place, working and effective and thus reducing the risk grading.
- Planned or work in progress to address potential gaps in control and thus will reduce the risk grading once implemented.

4.6.3 Assurance on Controls - How do we know that are controls are sufficient and effective?

4.6.4 Identifying the gaps in controls and assurances on controls aids the identification of actions that are needed to improve the mitigation of risks.

4.6.5 The best course of action is to employ either one or a mix of the following mitigating actions:

- **Tolerate** - Where the level of the risk falls below the Council's risk appetite and a conscious decision is made to accept that level of risk and take no further action other than ongoing monitoring and periodic review.
- **Terminate** – Avoid or eliminate the risk by for example withdrawing from a particular activity, project or service.
- **Treat** – Take action to reduce the level of risk by reducing either the impact or the likelihood of the risk event occurring. Impact can be reduced Detective controls and likelihood by Preventative controls.
- **Transfer** – By involving a third party to bear the whole or part of the risk through insurance.

4.6.6 Risk Management is more effective when a combination of preventative and detective internal controls are used to treat the risk.

4.6.7 In choosing between these responses, factors to consider include cost, feasibility, probability and the potential impact. Every control has an associated cost and it is important that the control action offers value for money in relation to the risk that it is controlling.

### 4.6.8 Preventative Controls

4.6.9 Preventive controls protect the organisation against specific risks and are stronger than controls that detect something after it has happened. Examples of preventative controls include:

- Standards, Policies and Procedures such as Financial Regulations
- Segregation of duties so that no one is in control of the whole of a transaction
- Authorisation rights reflecting level of responsibility
- Physical security of valuables by use of safes, keys, and room access controls
- Computer passwords, access controls, and file locks, to prevent unauthorised electronic access. Also, Firewalls and network controls

- Structured training and other programmes
- Robust contract and project management arrangements
- Setting budgets
- Benchmarking
- Job rotation, enforced vacations etc. to reduce chances of long-term fraud.

### 4.6.10 Detective Controls

4.6.11 Detective controls help management identify when preventative controls have broken down and corrective action is needed. For example:

- Supervisory review and sign-off of accounting work, expense reports, expenditure reports, payroll data, etc.
- Surprise cash counts
- Management review
- Budget monitoring
- Reconciliation between records such as income received and income banked
- Maintenance of records of stocks/assets followed by regular stock checks
- Exception reporting and resolution to highlight out-of-the-norm items

4.6.12 Another factor to consider is the opportunity to exploit the positive impact that might arise whenever tolerating, treating or transferring a risk i.e. where the potential gain seems likely to outweigh the potential downside.

### 4.7 Target Risk Assessment

4.7.1 Once the actions to further mitigate the risk have been identified a second risk assessment should be carried out. This time the risk assessment is carried out as if all the actions had been completed, reflecting how the planned actions would have reduced the overall risk rating.

## 5. Opportunity Risk

5.1 Opportunity risk is defined as a 'failure to identify or exploit an opportunity which is unable to be pursued later without an additional cost'. Managing opportunity risk involves creating a fertile climate for innovation in which an awareness of the constraints doesn't stop people coming up with ideas and putting them forward.

5.2 Risk and opportunity go hand in hand. The opportunity for advancement cannot be achieved without taking risk and risk is essential to progress and innovation. Excessive

caution can be as damaging as unnecessary risk taking and failure is often a key part of organisational learning.

## 6. Reviewing and Reporting

6.1 Procedures are in place to gain assurance over the efficacy of the Risk Management framework through regular review to ascertain whether:

- risks are still relevant
- emergent risks have been identified
- likelihood and impact of risks has changed
- Controls are still effective

6.1.1 The Council is the governing body of the GPhC and determines the governance policy and framework for the organisation. The Council conducts an annual risk management review and reviews the SRR four times per year. This review is informed by a risk review paper prepared by the chief executive, based on discussions within the Executive, which draws on the SRR, highlighting how the strategic risks are being managed including changes since the previous report. The Chief Executive's paper to the Council also includes a summary of the Audit and Risk Committee's most recent view of the efficacy of the Risk Management framework operating within the organisation and any specific comments on the strategic risks.

6.1.2 The Audit & Risk Committee supports the Council by reviewing and advising the Council on the operation and effectiveness of the arrangements which are in place across the whole of the Council's activities that support the achievement of the Council's objectives. The Committee meets four times per year to review the organisation's SRR and risk management arrangements.

6.1.3 In particular, the Committee scrutinises, on behalf of Council, the adequacy of:

- All risk and control related disclosure statements, together with any accompanying internal audit statement, external audit opinion or other appropriate independent assurances, prior to endorsement by the Council;
- The underlying assurance processes that indicate the degree of the achievement of corporate objectives, the effectiveness of the management of principal risks and the appropriateness of the above disclosure statements;

6.1.4 The Executive receives regular reports on the progress of the Risk Management framework and the make-up of and movement in the Strategic Risk Register.

6.1.5 Appendix C provides a high-level schedule of the risk management activities that occur throughout a calendar year.

6.1.6 Risks and risk registers at a directorate/service level are reviewed as part of the routine cycle of team meetings. The review can be evidenced by including Risk Management as a standing on the agenda prepared for each meeting.

### 6.2 Risk Appetite

6.2.1 Risk appetite is defined as: 'the amount of risk an organisation is prepared to take in pursuit of its objectives'. The principle recognises that risk cannot be reduced to zero and that mitigation will have both resource and cost implications. All successful organisations need to be clear about their willingness to accept risk in pursuit of their goals.

6.2.2 Risk appetite and risk tolerance are inextricably linked to performance over time. While risk appetite is about the pursuit of risk, risk tolerance is about the level of risk the organisation can reasonably deal with. This dual focus on taking risk and exercising control is both innovative and critical. The innovation is not in looking at risk and control, it is in looking at the interaction of risk and control as part of determining risk appetite.

6.2.3 The concept of a "risk appetite" is key to achieving effective risk management and it is essential to consider it before moving on to consideration of how risks can be addressed. The concept may be looked at in different ways depending on whether the risk being considered is a threat or an opportunity:

- When considering threats the concept of risk appetite embraces the level of exposure which is considered tolerable and justifiable should it be realised. In this sense it is about comparing the cost (financial or otherwise) of constraining the risk with the cost of the exposure should the exposure become a reality and finding an acceptable balance;
- When considering opportunities the concept embraces consideration of how much one is prepared to actively put at risk in order to obtain the benefits of the opportunity. In this sense it is about comparing the value (financial or otherwise) of potential benefits with the losses which might be incurred (some losses may be incurred with or without realising the benefits).

6.2.4 The capacity of the GPhC to determine its own risk appetite is constrained by its nature as a regulatory body. GPhC has limited scope to decide not to do things, as it has to continue to deliver on its legal obligations.

6.2.5 The GPhC's work on risk appetite is considered by the Executive Team and forms part of the assurance reporting to the Audit and Risk Committee. The Council ultimately approves the organisation's Risk Appetite Statement.

6.2.6 Risk management should interact dynamically with objective-setting, with risk management activity sometimes usefully highlighting the need to review the organisation's objectives, as well as being informed by them.

6.2.7 Actions for each risk should seek to resolve any gaps in control or assurance on controls.

## 7. Enterprise Risk Management (ERM)

7.1 ERM is an holistic approach to managing risk exposures across the entire organisation. Both ISO 31000: 'Risk Management Principles & Guidelines' and BS31100: Code of Practice for Risk Management espouse the use of ERM as it helps address the entire management system – from design, implementation and maintenance to the improvement of risk management processes.

7.2 The following initiatives will help further align GPhC to the fundamental principles of an ERM framework

### 7.3 JCAD Risk & Incident Management Software

7.3.1 JCAD Version 4 is GPhC's Risk & Incident Management software which enables a consistent and structured approach to the management of threats and opportunities across the organisation. The application allows officers to link risks to the delivery of the Councils aims and objectives. The application is aligned to ISO:31000 and BS: 31100.

7.3.2 The integrated software enables:

- Real time visibility of all risks and risk registers across the organisation.
- Version control over documents;
- Movements between operational risk registers and the Strategic Risk Register.
- 'Out of date' risk triggers to help ensure risks are regularly reviewed and updated.
- The maintenance of a complete and up-to date audit trail.

### 7.4 Corporate Risk Management Forum (CRMF)

7.4.1 The aim of CRMF, which will meet quarterly, is to help drive good practice, embed principles and coordinate all aspects of risk management focussing on operational and cross cutting issues.

7.4.2 The Forum will help support adherence to the Risk Management Policy, empower colleagues to manage risks and thus contribute to the achievement of GPHC's strategic objectives.

### 7.5 Incident Management

7.5.1 An incident can be defined as an event or circumstance which could have resulted (near miss), or did result, in:

- Unnecessary damage, loss or harm to patients, staff, visitors or members of the public, registrants and pharmacy premises.

- A reduction in GPhC's ability to continue to deliver services, for example actual or potential loss of personal/organisational information, damage to property, the environment or IT failure.
- Adverse media coverage and damage to the reputation of the organisation.

7.5.2 An incident may be the result of a risk that has materialised and this direct link allows for it to be recorded and reported through the integrated JCAD Risk & Incident Management software. Further guidance on this subject is provided within the Incident Management Reporting & Learning (IMRL) Framework document.

7.6 **Staff Training & Development**

7.6.1 A rolling program of monthly briefing sessions on the fundamental principles of Risk Management has been developed and delivered to colleagues.

7.6.2 Practical training on the JCAD Risk software is also available to relevant colleagues.

8. **Links with other Processes**

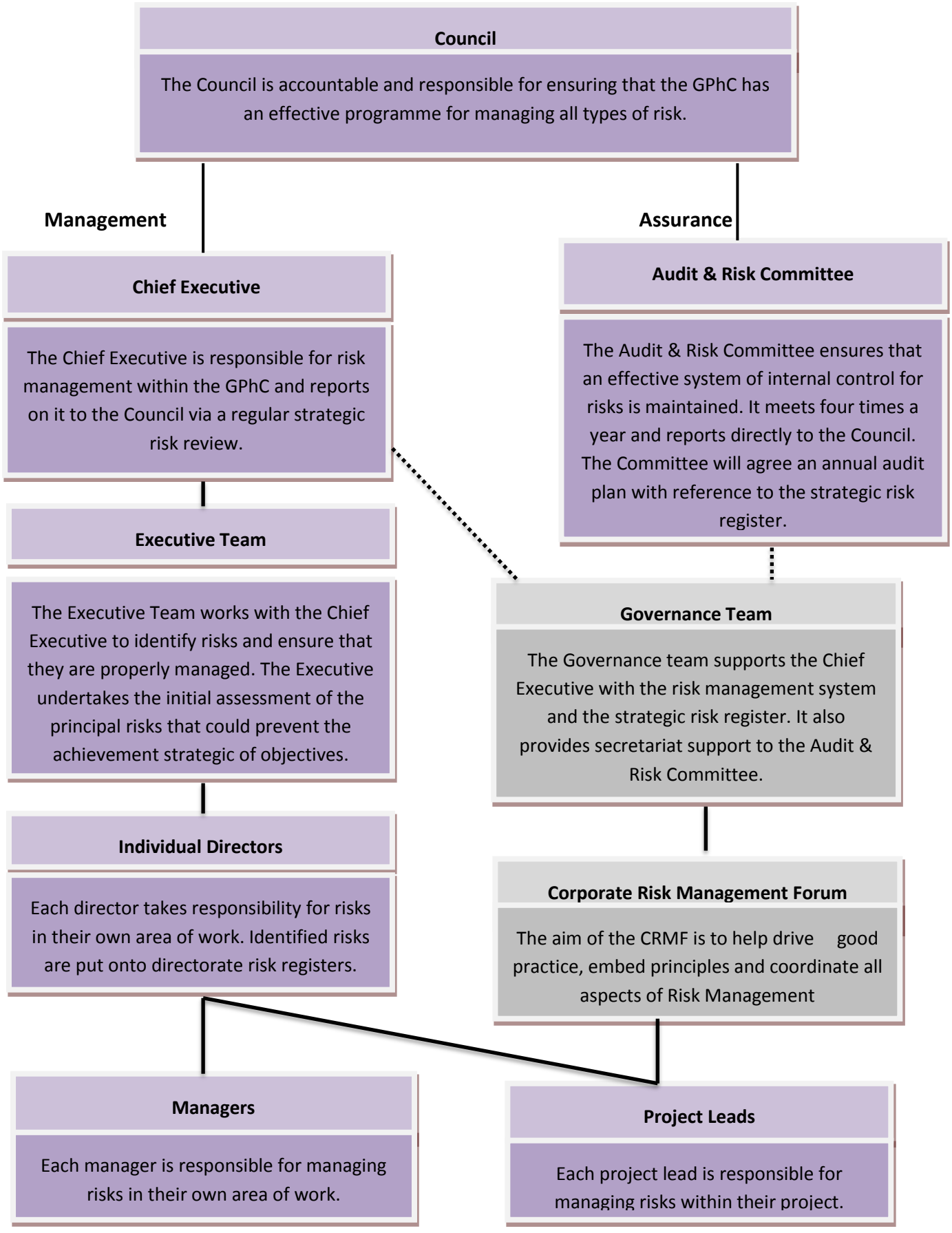
8.1 The chief executive uses the risk register to inform objective setting and performance management with members of the executive team. The risk register is also used to integrated with strategic and business planning and the Council agenda-setting. This ensures that the Council's attention and effort in a particular area is proportionate to the risks in that area.

9. **Measurement and Evaluation**

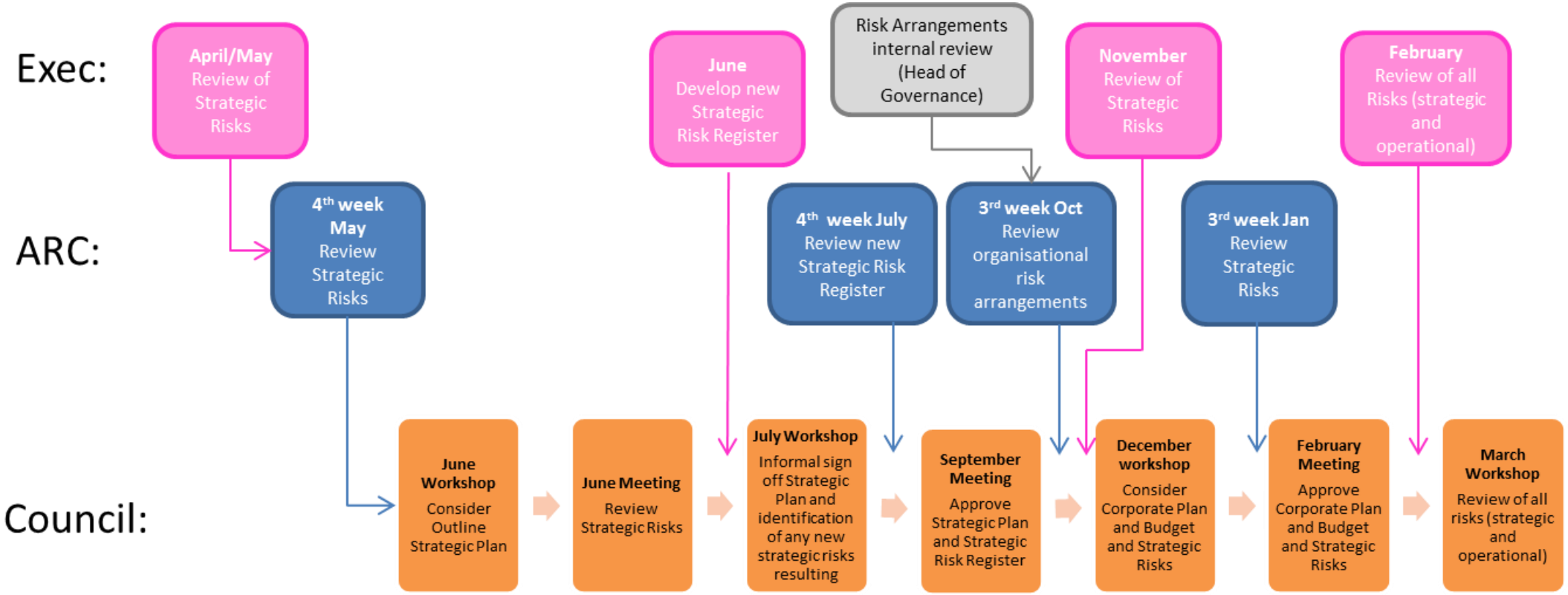
9.1.1 The Risk Management Policy will be reviewed annually to ensure that it meets the organisations objectives and that alignment to contemporary risk management standards is maintained.

**Matthew Hayday, Head of Governance**
**Reference:** GP/2015/106
**Effective date:** 01 July 2015
**Review date:** 01 July 2017
**Agreed by:** Agreed by email by Duncan Rudkin 26/06/2015

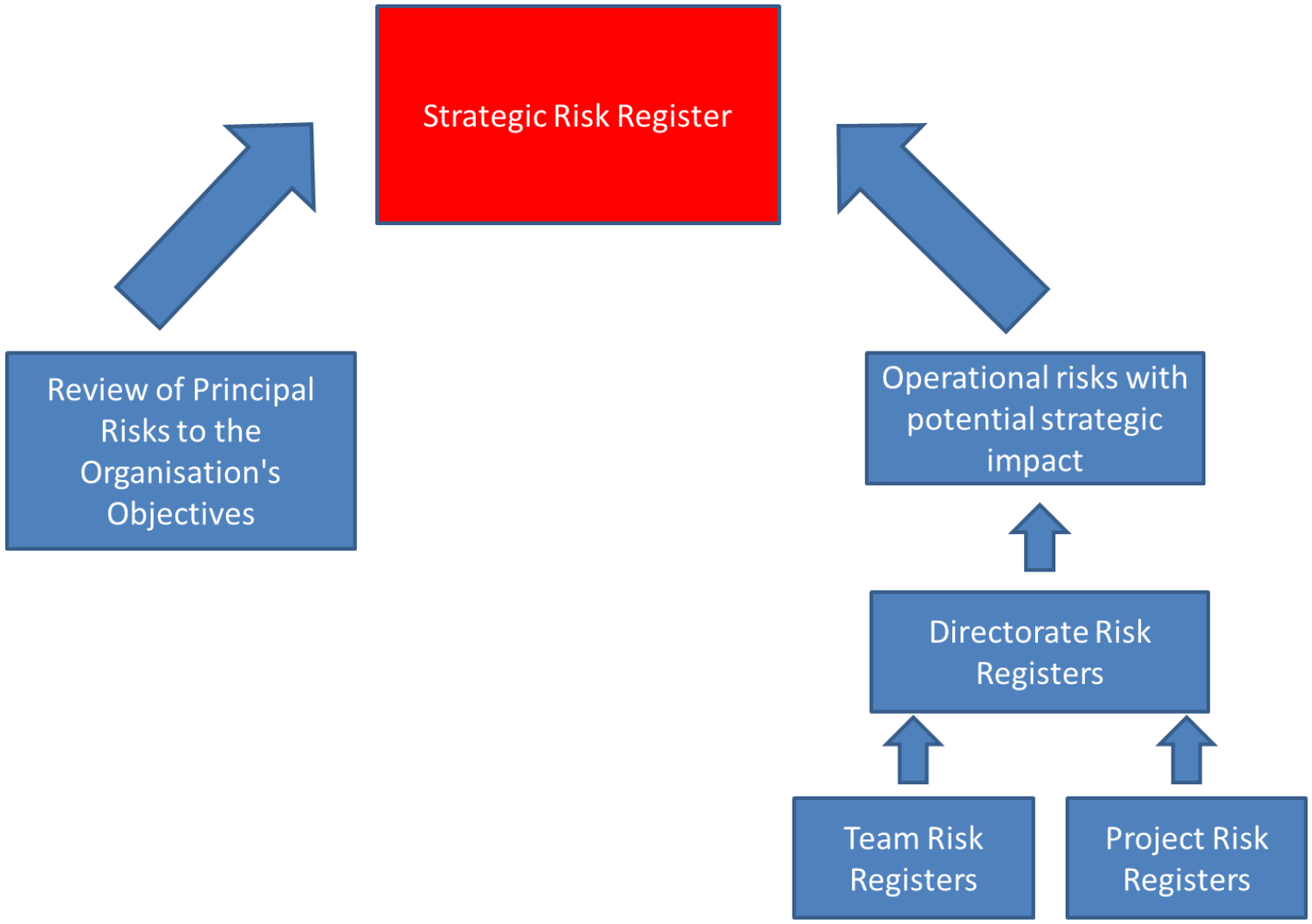
## Appendix A – The organisational structure for risk management and assurance



**Appendix B – Strategic Risk Cycle**



## Appendix C – Escalation to the Strategic Risks Register



## Appendix D Risk Assessment - Impact, Likelihood & Profiling

| Impact | | | | | |
|---|---|---|---|---|---|
| **DESCRIPTOR** | **1 INSIGNIFICANT** | **2 MINOR** | **3 MODERATE** | **4 MAJOR** | **5 CATASTROPHIC** |
| **Financial (damage/loss)** | Organisational / financial loss (£< 1k) | Organisational / financial loss (£1,000-£10,000) | Organisational/financial loss (£10,000 - 100,000) | Organisational / financial loss (£100,000 - £1m) | Organisational / financial loss (£>1m) |
| **Reputation & publicity** | Limited negative local public exposure with negligible impact on stakeholder confidence. | Negative local public exposure with low impact on stakeholder confidence. Local media coverage <1day | Negative local and limited national public exposure with moderate impact on stakeholder confidence and PSA concern. | Negative national public exposure with significant impact on stakeholder confidence. Loss of public confidence. | Full public inquiry. MP concerns/ questions in parliament. Severe loss of confidence in the organisation. |
| **Information Governance** | **Potential** breach of confidentiality risk assessed as low, e.g. files/data was encrypted | Serious **potential** breach of confidentiality e.g. unencrypted records/data lost. | Serious breach of confidentiality from inadequately protected PC(s), laptop(s) and remote device(s) | Serious breach of confidentiality with particularly sensitivity data. | Serious breach of confidentiality with potential for ID theft. |
| **Information Technology** | An event which leads to loss of critical business processes but can be managed under normal circumstances and resolved quickly and easily | An event which leads to loss of critical business processes but can be managed under normal circumstances and resolved in around 1 day | A significant event, which leads to loss of critical business processes but can be managed under normal circumstances and resolved in 1 or 2 days. | A critical event, which leads to loss of critical business processes, but can be resolved with proper management within a few days. | An extreme event, which leads to loss of critical business processes which takes significant management time and resources to resolve. |
| **Legislative** | Minor internal breach | Significant internal breach | Reportable incident to regulator, no follow up | Report of breach to regulator with immediate correction to be implemented | Report to regulator, prosecution or fines requiring major corrective action |

| Impact | | | | | |
|---|---|---|---|---|---|
| **DESCRIPTOR** | **1 INSIGNIFICANT** | **2 MINOR** | **3 MODERATE** | **4 MAJOR** | **5 CATASTROPHIC** |
| **Security** | Very minor incidents/ damage to assets, property or personnel | Localised incidents/ damage to assets, property or personnel with no effect on service delivery | Organisational wide incidents/ damage to assets, property or personnel with some effect on service delivery | Organisation wide incidents/ damage to assets, property or personnel with significant impact on service delivery. | Extreme incident with major effects on the organisation's ability to deliver core services. |
| **Health & Safety** | On-site exposure, immediately contained. Trivial injury | On-site exposure, contained after prolonged effect . Minor injury | On-site exposure, contained with outside assistance. Major injury | Prolonged/Major incident with serious casualties. Major injuries | Major incident with fatalities |
| **Staffing and Competence** | Short term low staffing level temporarily reduces service quality (< 1 day) | Ongoing low staffing level reduces service quality. **Minor error** due to ineffective training. | Late delivery of key objectives/service due to lack of staff. **Moderate error** due to ineffective training. | Uncertain delivery of key objectives / service due to lack of staff. **Major error** due to ineffective training | Non-delivery of key objectives / service due to lack of staff. Loss of key staff **Critical error** due to ineffective training. |
| **Projects** | Minimal impact on project | Delay/ minor issues with project, but within tolerances | Delay or issues with project outside of tolerances | Uncertain delivery of project | Non-delivery of project |

**LIKELIHOOD – A guide to evaluating the likelihood of identified risk occurring**

**Risk Assessment - Likelihood**

| Likelihood | Score | Rationale |
|---|---|---|
| Almost Certain | 5 | Once in 12 months |
| Likely | 4 | Once in 2 years |
| Possible | 3 | Once in 5 years |
| Unlikely | 2 | Once in 10 years |
| Rare | 1 | Once in over 10 years |

**Risk Profiling -** Using the outputs from the risk assessment process, a profiling exercise should be undertaken to determine its level (score). This is an important step as it identifies priorities for further action. The individual risk scores are then plotted onto a risk profile matrix to enable clear and easy comparisons to be made with other risks:

**RISK MATRIX – L**ikelihood x Impact

| GPhC Risk Matrix | | I M P A C T | | | | |
|---|---|---|---|---|---|---|
| | | 1 Insignificant | 2 Minor | 3 Moderate | 4 Major | 5 Catastrophic |
| LIKELIHOOD | 5 Almost Certain | 5 | 10 | 15 | 20 | 25 |
| | 4 Likely | 4 | 8 | 12 | 16 | 20 |
| | 3 Possible | 3 | 6 | 9 | 12 | 15 |
| | 2 Unlikely | 2 | 4 | 6 | 8 | 10 |
| | 1 Rare | 1 | 2 | 3 | 4 | 5 |

**RISK RATING** – for grading risk, the scores obtained from the risk matrix are assigned grades as follows

**Risk Assessment - Profiling**

| Rating | Risk Description | Action |
|---|---|---|
| 15-25 | Extreme | Immediate further action required & review monthly |
| 8-12 | High | Review risk and control actions on a quarterly basis |
| 4-6 | Medium | Monitor and review on a 6 monthly basis) |
| 1-3 | Low | |