PUBLIC
C29(19)

COUNCIL

GOC's Risk Management Policy

Meeting: 10 July 2019 **Status:** for decision
Lead responsibility & paper author: Mark Webster (Director of Resources)

Purpose

1. To present the revised Risk Management Policy.

Recommendations

2. Council is asked to **consider** and **approve** the updated Risk Management Policy.

Strategic objective

3. An effective risk management policy is fundamental to the achievement of all the GOC's strategic objectives and is an essential part of good governance.

Risks

4. Risk management is a key element of the management of GOC's affairs and operations. Being able to identify and where possible mitigate risk is key to ensuring the organisation can continue to fulfil its statutory duties.

Background

5. The risk management policy was originally agreed and adopted by Council in January 2013

6. Effective risk management has been a subject of discussion at ARC since the new committee members joined and much work has been undertaken to embed risk management into the organisation. The comprehensive revision of the policy is the last part of this work.

Analysis

7. The revised risk management policy is presented in full at **annex one**.

8. With the exception of the table in **section seven** regarding risk appetite this policy was reviewed and discussed at ARC at its meeting on 9 May 2019.

9. The table for risk appetite was subsequently completed in full capturing Council's thoughts and comments from the recent review day, combined with a similar exercise carried out by the Executive.

10. The updated risk management policy was discussed at ARC at its recent meeting on 28 June 2019 at which the committee agreed to recommend to Council that the revised Risk Management Policy is approved.

Impacts

11. No implications have been identified in relation to reserves, budget, legislation, resources, equality, diversity and inclusion, Human Rights Act or sustainability.

Devolved nations

12. No implications/differences in relation to this area and the devolved nations have been identified.

Communications

13. The risk management strategy and policy will be circulated to staff once Council has approved it.

Timeline for future work

14. This policy will go to Council for approval on 10 July 2019.

Attachments

Annex one - draft revised risk management policy.

C29(19) – ANNEX ONE

TITLE	Risk Management Strategy and Policy
VERSION	Version 3
SUMMARY	The policy provides the framework for the management and control of risk within the GOC
DATE CREATED	January 2013
REVIEW DATE	June 2019
OWNER	Mark Webster - Director of Resources
APPROVED BY	Audit & Risk Committee

Contents Page

Section	Description	Page
1.	Policy statement	3
2.	Risk management objectives	3
3.	Responsibilities & Accountabilities	4
4.	Risk Registers	4
5.	Risk management process	5
5.1	Risk identification	5
5.2	Risk analysis	7
5.3	Risk recording and monitoring	10
6.	Response to risk	10
7.	Risk appetite	11
8.	Ongoing management and review	13

1. 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 regulation. It is therefore an essential part of good governance that we manage these risks effectively.

The General Optical Council's Risk Management Policy is to adopt best practice in the identification, evaluation and cost-effective control of risks, to ensure that they are reduced to an acceptable level.

GOC's Risk Management strategy is to:

1. Embed risk management into corporate processes including financial and strategic planning;
2. Manage risk in accordance with best practice;
3. Consider legal and regulatory compliance as an absolute minimum;
4. Anticipate and respond quickly to legislative, environmental and operational change;
5. Prevent injury and damage and reduce the cost of risk.

Risk management is the process of identifying significant risks to the achievement of the organisation's strategic and operational objectives, evaluating their potential consequences and implementing the most effective way of controlling them.

The process also clearly identifies who is responsible for monitoring and managing particular elements of the risk management cycle; how this is reported; to whom; and most importantly how any emerging issues perceived to have an impact on the GOC's risk profile are acted upon and escalated.

2. Risk Management Objectives

The objectives set out above will be achieved by:

1. Ensuring that the identification and management of risk is owned by the Senior Management Team and Heads of Department, with appropriate review and reporting structures.
2. Including risk as an item for regular discussion and review at monthly SMT / Leadership Team meetings and committees.
3. Including all staff in the identification of risk, and review of the risk profile for their area of the organisation through regular discussion and review at team meetings.
4. Provide training in risk awareness and where appropriate, risk management.
5. Maintaining documented procedures for the control of risk which are regularly reviewed and updated.
6. Ensuring that where risk is identified, that appropriate mitigation is put in place to manage risk, and where this is not possible, that this is itself noted and reviewed.
7. Monitor arrangements on an on-going basis and undertake a formal review of this policy and its associated procedures at agreed timely intervals.
8. The use of a structured, targeted risk assurance framework.

3. Responsibilities and Accountabilities

Every member of the GOC has a responsibility to help manage risk across the organisation. To ensure that risk strategy remains central to the management of the organisation, the following groups will have specific responsibility for risk in the areas described above.

Council will have an overall responsibility to ensure the implementation of an appropriate risk management strategy, supported by appropriate structures and processes, and to provide sufficient resources to meet agreed objectives.

The Audit & Risk Committee has a critical scrutiny role in relation to the periodic review of the most significant risks facing the GOC.

The Senior Management Team has responsibility for the day to day assessment of corporate level risks and for ensuring that risk assessments are regularly updated, and summary reports presented to the Audit & Risk Committee for review. SMT should periodically review directorate level risk registers and provides a collective challenge to updated risk analyses.

The Director of Resources has responsibility for maintaining an up-to-date Corporate Risk Register and for advising Council and SMT on its risk policies and procedures.

Directors are each responsible for ensuring that proper procedures are in place to effectively identify, evaluate and manage risks within their directorates, for maintaining an up-to-date Directorate Risk Register and for the periodic review and update of departmental risk registers.

The Leadership Team is responsible for highlighting new, emerging or heightened risk at the earliest opportunity and for periodically reviewing the Corporate Risk Register.

Heads of Department are each responsible for ensuring that proper procedures are in place to effectively identify, evaluate and manage risks within their service areas and for the periodic review and update of departmental risk registers.

Project leads are responsible for maintaining project risk registers, including risks that may need to be managed in another part of the organisation.

Individual managers and employees are responsible for the effective management of the risks associated with their particular roles and duties, and for ensuring that significant risks are identified to heads of department or senior management as soon as they become known.

4. Risk Registers

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

The **Corporate Risk Register (CRR)** 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 CRR are identified through the Executive's assessment of the risks to the organisation's Strategic Plan. This exercise is reviewed by 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 CRR. The CRR is maintained by the Director of Resources on behalf of the Chief Executive and is presented in its entirety to the Audit & Risk Committee at every meeting.

Directorate Risk Registers provide a record of the most significant operational risks facing each directorate. These registers will be periodically reviewed by SMT collectively and risks with strategic implications and/or high scores should be escalated to the Corporate Risk Register. Well managed risks can be de-escalated to departmental or project risk registers when appropriate.

Departmental Risk Registers record the detailed risks at individual project, team or departmental level. Risks that have strategic implications and/or have high scores should be considered for escalation to the Directorate or Corporate Risk Registers.

Project Risk Registers provide a record of the risks that have been identified from individual projects. Project risks can be escalated to either Directorate Risk Registers or the Corporate Risk Register via the relevant director. There are three criteria for the escalation of project risks: a high risk score, a risk score that may not be high, but that exceeds project tolerance levels and dependencies between projects that cannot be managed at the project level.

5. Risk Management Process

The basic principles of risk management are the identification, analysis, control and monitoring of risks. The processes associated with these are: -

5.1 Risk Identification

In order to enable risk to be effectively managed, the nature of the risk must first be identified.

Risks may be identified from a variety of sources, including:

- The Strategic Plan
- The annual business plan (particularly in relation to significant projects)
- Stakeholder feedback
- External and internal audits and reviews
- Changes to the legal, regulatory, political and environmental landscapes.

Risks are categorised into the following areas, and staff will be trained in identifying risks in these accordingly.

Type	Risk Definition	Examples
Political	Changes in Government policy.	• Inappropriate strategic priorities • Poor horizon scanning. • Inability to modernise/innovate.
Financial	Ability to meet Council's financial commitments.	• Missed business opportunities • Material misuse of resources or fraud • Poor financial data
Social	Social factors affecting the ability of the Council to deliver strategic objectives.	• Demographic change • Shortage of trained staff. • Capability & capacity issues
Technological	Failure to keep pace with technological change.	• Obsolescence • Increase downtime • Major IT or project failure
Legislative and Regulatory	Ability to manage current changes in UK and/or EU law/regulation	• Significant breaches of statutory legislation. • Failure to follow internal policies and procedures. • Inadequate response to legislative changes
Customer	Ability to meet changing customer needs and expectations.	• Poor stakeholder management • Dissatisfied customers • Poor Image

Additional factors in risk identification:

• The nature and complexity of activity undertaken.
• General financial health and the level of reserves available to absorb financial risks.
• The adequacy of internal control systems.
• The GOC's vulnerability to external factors outside its control.
• The skills set of employees and council.
• The adequacy of business continuity plans.

5.2 Risk Analysis

Once risks have been identified and categorised they are assessed in terms of their likelihood and their potential impact on the GOC at a departmental, directorate and corporate level using the method below.

Risk Definition & Description

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.

Risk Ownership

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 CRR must be assigned to a member of the Senior Management Team as the owner. Risks on Directorate Risk Registers should be assigned to a member of the Directorate Management Team.

Risk Assessment

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).

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.

Based on this assessment, the risks which require the greatest level of management can be identified, i.e. those with a high likelihood of occurrence and a major impact on the GOC.

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		
Scoring		
1	Very Low	Under 1% chance of occurrence in next 12 months
2	Low	1%-10% chance of occurrence in next 12 months
3	Medium	11%-25% chance of occurrence in next 12 months
4	High	26%-50% chance of occurrence in next 12 months
5	Very High	Over 50% chance of occurrence in next 12 months

5.3 Risk Recording and Monitoring

Each risk register should contain the following information:

- Risk Identified
- Type of Risk
- Risk owner
- Action
- Impact and Likelihood scores at inherent risk level, and overall score
  - Inherent risk is the initial assessment of the GOC's risk exposure of the particular risk identified.
- Summary of existing key controls and mitigations.
- Impact and Likelihood scores at current risk level, and current overall risk score.
  - Current risk is the assessment of the GOC's risk exposure of the particular risk identified after taking into account the existing key controls and mitigations.
- What actions are proposed to further reduce the level of residual risk.
- Responsible executive.
- Impact and Likelihood scores at target risk level, and target overall net risk score
  - Target risk reflects the level of the GOC's acceptable risk exposure of the particular risk identified after taking into account the proposed actions to improve key controls and mitigations.
- Direction of travel – is the net risk position improving, worsening or the same as at the last assessment

The risk register should be maintained on a regular basis by updating it to reflect changes to existing risks and for inclusion of any significant new risks identified, whilst maintaining an audit trail of changes.

6. Response to risk

Once risks have been identified, the risk profile will be managed using the following methods.

- **Avoid -** Risk avoidance involves changing aspects of the identified risk to eliminate the threat. Risks that are identified early may be avoided by clarifying requirements, obtaining more information, improving communications, or obtaining expertise.

- **Transfer -** Risk transference involves shifting the negative impact of a threat (and ownership of the response) to a third party. Risk transference does not eliminate a threat; it simply makes another party responsible for managing it. If that is the strategy, then the party to whom the risk is being transferred must be informed and accept responsibility for that transfer. Any disputes should be escalated to the relevant Director and if necessary, SMT.

- **Mitigate -** Risk mitigation involves reducing the probability and/or the impact of risk threat to an acceptable level. Taking early and pro-active action against a risk is often more effective than attempting to repair the damage a realized risk has caused. Developing contingency plans should be considered for risks that remain high despite mitigation.

- **Accept -** Acceptance is often taken as a risk strategy since it is very difficult to plan responses for every identified risk. Risk acceptance should normally only be taken for low-priority risks. Risk acceptance can be passive, where no action is taken at all, or active.

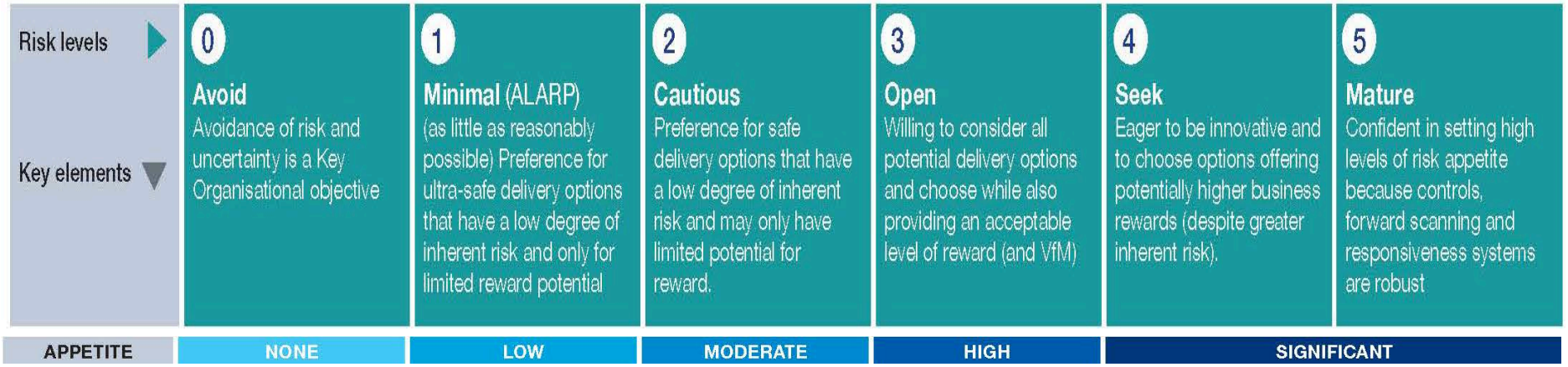
7. Risk Appetite

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.

The risk appetites below recognise that different tolerances may be applied in identifying and managing different risks and should guide decisions on what is the right level of control across the organisation. These can also help management determine the required systems and controls that are commensurate with the level of operational risk it is willing to accept.

The GOC has determined that the following appetite for risk, or tolerance levels, are appropriate in relation to the following types of risk:

Type	**Level 0-5**	**Comments**
Political	4	We need to be willing to assert our independence in dealings with stakeholders and if necessary take on a higher level of risk to achieve our strategic objectives.
Financial	2	We are the custodian of registrant's money and recognise the need to deliver value for money, so should be cautious about financial risk.
Capability & Capacity	3	As a relatively small organisation with finite resources, we may not have specialist expertise to cover all areas, meaning we should be open to taking some risks in this area.
Technological	4	Being innovative in using technology to support our objectives will involve greater risk, reflecting the inherent risk of all technology challenges.
Data Security	1	Dealing with highly sensitive personal data means we should avoid risk in this area.
Legislative & Regulatory	2	As a regulator we must demonstrate high standards and therefore be cautious about legislative and regulatory risk.
Customer Service	3	Public protection is our number one priority and that will sometimes involve un-popular decisions.
Casework	3	We recognise that we have to challenge and drive change in order to improve our efficiency and effectiveness, which will involve being open to taking some, managed risks.


Risk levels
Key elements
0
Avoid
Avoidance of risk and uncertainty is a Key Organisational objective
1
Minimal (ALARP)
(as little as reasonably possible) Preference for ultra-safe delivery options that have a low degree of inherent risk and only for limited reward potential
2
Cautious
Preference for safe delivery options that have a low degree of inherent risk and may only have limited potential for reward.
3
Open
Willing to consider all potential delivery options and choose while also providing an acceptable level of reward (and VfM)
4
Seek
Eager to be innovative and to choose options offering potentially higher business rewards (despite greater inherent risk).
5
Mature
Confident in setting high levels of risk appetite because controls, forward scanning and responsiveness systems are robust
APPETITE
NONE
LOW
MODERATE
HIGH
SIGNIFICANT

8. On-going Management and Review

For any risk management system to work effectively – including the key components outlined within this Risk Strategy – there must be a clear commitment to regular and on-going review, challenge and refreshing of the content of corporate, departmental and departmental risk registers accompanied by a regularised cycle of reporting, and scrutiny at Audit Committee and Council level.

These reviews should ascertain whether:

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

The review of the GOC risk registers takes place on the following basis

Group	Frequency	Comments
HOD's and Director	Monthly	Review the departmental risk registers and identify risks that may need to be raised to the departmental register.
HOD's and Director	Monthly	The group will review the departmental risk registers and identify risks that may need to be raised to the corporate register.
Leadership team	Monthly	Risk will be a standing item on each agenda with the focus on any new areas of concern.
SMT	Monthly	Risk will be a standing item on each agenda; the group will review the corporate risk register and add or remove items based on that discussion and the review of departmental risks registers.
Audit & Risk Committee	Quarterly	Audit Committee will review the corporate risk register with the potential to review a particular strategic risk at each meeting.

Council	Quarterly	Will receive assurance from ARC with the potential to review a particular strategic risk at each meeting if deemed appropriate.
Internal Auditors	Annually	The risk register and risk management process will be reviewed on an annual basis by the appointed internal auditors. Recommendations for changes to the process will be agreed with SMT and the Audit Committee.

RISK MATRIX – Likelihood x Impact

Risk Matrix		I M P A C T				
		1 Insignificant	2 Minor	3 Moderate	4 Major	5 Catastrophic
	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

Escalation to the Corporate Risk Register