Annex 1

TITLE	Risk Management Strategy and Policy
VERSION	Version 2
SUMMARY	The policy provides the framework for the management and control of risk within the GOC
DATE CREATED	January 2013
REVIEW DATE	January 2016
OWNER	Josie Lloyd - Director of Resources
APPROVED BY	

Contents Page

1. Policy Statement

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 either eliminated or reduced to an acceptable level.

GOC's Risk Management strategy is to:

1. Integrate risk management into the culture of the organisation;
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; and
6. Raise awareness of the benefits of effective risk management in supporting the achievement of objectives.

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.

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 senior managers and Heads of Department, with appropriate review and reporting structures.
2. Including risk as an item for regular discussion and review at relevant meetings and committees.
3. Including all staff in the identification of risk, and review of the risk profile for their area of the organisation.
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.

3. Responsibilities

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 Committee has a critical scrutiny role in relation to the periodic review of the most significant risks facing the GOC, which may be cross-organisation corporate level risks or major risk emerging from within specific departments.

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 Committee for review. SMT periodically reviews departmental level risk registers and provides a collective challenge to updated risk analyses. Within GOC, Executive leadership is provided by the Director of Resources.

Departmental heads 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.

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

4. Risk Management Process

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

4.1 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 in the following areas, and relevant staff will be trained in identifying risks in these accordingly.

Risk Category	Examples	GOC possible outcomes
Governance	• Organisational structure inadequate or inappropriate • Trustees lack skills • Conflicts of interest	• Poorly skilled leaders make poor decisions • Council lacks skills to oversee strategic direction effectively • Reputational damage as result of perceived conflict of interest in decision-making (e.g. Specsavers story)
Operational	• Legal challenge • Poor contract pricing • Poor recruitment or training of staff • Security of assets	• Successful challenge and costs attached • Poor service provision, rising complaints or challenges • Key services cost more than anticipated or provide poor service • Poor quality ICT infrastructure does not support business • Assets lost or damaged
Financial	• Poor financial data • Inadequate reserves or cashflow • Limited income sources • Poor investment management • Insufficient insurance cover	• Poor decision-making around fees and budgets • Unable to keep pace with rising expectations of service users • Unable to keep pace with technological advances • Loss of assets/income uninsured
External	• Poor public perception • Demographic changes • Turbulent economic/political environment • Change in government policy	• Fundamental shift in expectations for regulators • Changes in numbers of registrants leading to pressure on fees • Economic pressure exerts pressure on fee levels
Compliance with law & regulation	• Breach of trust • Poor knowledge of legal responsibilities as employer • Poor knowledge of regulatory framework organisation operates within	• Registrants lose confidence in GOC using fees to best purpose • Organisation faces ETs (costly and reputational damage) • Organisation unable to meet requirements of regulator

4.2 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 department and corporate level using the method below.

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 or at departmental level.

The risk management methodology involves the utilisation of a scored risk matrix, which scores the likelihood of occurrence and the severity of impact, with the overall risk assessment being the two scores multiplied together. The following scoring process is currently utilised:

		Impact	Likelihood
1	**Very Low**	Cost less than £0.1M, minimal impact on reputation and no disruption to operation.	Under 1% chance of occurrence in next 12 months
2	**Low**	Cost £0.1M-£0.3M or limited impact on reputation or operation	1%-10% chance of occurrence in next 12 months
3	**Medium**	Cost £0.3M-£0.5M or some impact on reputation or operation	11%-25% chance of occurrence in next 12 months
4	**High**	Cost £0.5M-£1.0M or serious impact on reputation or operation	26%-50% chance of occurrence in next 12 months
5	**Very High**	Cost £1.0M or more, or catastrophic impact on reputation or operation	Over 50% chance of occurrence in next 12 months

If a risk is assessed as a high likelihood but low impact, the score will be 4 x 2 = 8. It follows that the higher the score out of a maximum of 25 the more important it is to ensure effective risk management arrangements are in place.

An example of the outcome of this scoring system is given below:

	Low Impact	**High Impact**
High Likelihood	**Score 5** High probability that this will happen, but little impact if it does, therefore action is dependent upon management being prepared to accept the consequences	**Score 25** High probability with big impact, needs careful managing

Low Likelihood	**Score 1** Little chance of it happening and little impact if it does, therefore no need for action	**Score 5** Little chance of it happening but if it does it will have a big impact, therefore needs some managing

The benefit of this approach is that it is relatively simple to understand and use and it will help to inform discussion about which risks are most significant and what action is required to address them.

4.3 Risk Recording and Monitoring

Risk registers are maintained on both a department and corporate level. The departmental risk register is the responsibility of each Head of Department, and is updated and reviewed with the relevant director on a monthly basis. The most significant risks identified by each department are then considered for inclusion in the corporate risk register held by the Head of Finance.

The corporate risk register is currently reviewed on monthly basis, whilst the process is bedding in, and new department risks are added where necessary. Significant changes to the risk profile will be identified to Council, and the Audit Committee will review the corporate risk register on a quarterly basis.

Each risk register contains the following information:

- Description of risk
- Risk owner
- Impact and Likelihood scores at inherent risk level, and overall score
- Summary of key controls and mitigations
- Impact and Likelihood scores at net risk level, and overall net risk score
- Direction of travel – is the net risk position improving, worsening or the same as at the last assessment?
- Overall Assessment – what assurance can be provided on the net risk position? Where are there currently gaps in control? Are there any emerging issues on the horizon that will impact on the risk assessment in the future?
- What actions are necessary in the next period aimed at further reducing the level of residual risk?

The risk register is being 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.

5. 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 can 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.

- **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 are examples of risk 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.

6. 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 and departmental risk registers accompanied by a regularised cycle of reporting, and scrutiny at Audit Committee and Council level.

The review of the GOC risk register takes place on the following basis and commenced from 15 October 2012.

Group	Frequency	Comments
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.
SMT	Monthly	Risk will be a standing item on each agenda.

SMT and HOD's	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 Committee	Quarterly	Audit Committee will review the corporate risk register at each meeting.
Council	Quarterly	Risk will be included in the quarterly performance report. Any significant new risks (and their mitigation) will be identified in this report for Council consideration
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.

This risk strategy will be reviewed by the internal auditors once appointed and any revisions will be made during the financial year 2013-14.