RISK MANAGEMENT POLICY AND STRATEGY

Effective: December 2025

To be reviewed: June 2029

To help the public service
spend wisely

TABLE OF CONTENTS

PURPOSE OF THE POLICY

1. The purpose of the risk management policy is to explain the Office of the Auditor General's ("OAG" or "Office") approach to risk management and to outline the key principles, strategies and responsibilities for the management of risk for the organisation.

OBJECTIVE OF RISK MANAGEMENT

2. The objective of undertaking risk management is to provide a systematic way of identifying, recording, monitoring and reporting on risks so that the OAG can manage its risks (through putting in place controls and mitigations) in order to meet its objectives.

PRINCIPAL POLICIES

3. The identification and management of risks affecting the OAG's ability to achieve its objectives as set out in the Office's Strategic Plan and other planning documents, such as Annual Budget Statements, are key responsibilities of all members of staff and partners involved in the OAG's work.

4. The effective management of risk is an important means by which the OAG achieves its goals. To that end the OAG's policies are to

    - manage risk actively across the full range of the OAG's activities;
    - devolve responsibility for risk ownership and management to the most appropriate level whilst maintaining clear senior management overall responsibilities;
    - integrate risk management with corporate planning;
    - encourage a risk aware way of working;
    - accept levels of risk that are compatible with our professional responsibilities and take into account stakeholder expectations; and
    - monitor and report regularly on the management of risk.

NATURE AND CONTEXT OF RISK

5. Risk can be defined as the threat that an event, action or inaction will adversely affect the OAG's ability to achieve its objectives.

6. Risks can be strategic or operational in nature and the OAG will be able to control some risks, influence others but only mitigate the impact of those risks that are outside of its control or influence. Risk management takes these factors into account in judging the acceptable level of risk and the actions needed to reduce the risk level.

STRATEGY FOR IMPLEMENTING THE RISK MANAGEMENT POLICY

ROLES AND RESPONSIBILITIES

7. Risk management is an integral part of the overall governance arrangements of the OAG. As such there are specific responsibilities for people and groups undertaking different roles in the Office.

Auditor General

8. The Auditor General has ultimate responsibility for the management of risk within the OAG. His/her role includes:

- setting the tone at the top for risk management throughout the organisation;
- approving the overall risk management arrangements including this policy and the appetite for risk; and
- considering reports on the operation of risk management.

Corporate Management Team

9. The Corporate Management Team (CMT) has day-to-day responsibility for the management of the system of internal control including risk management. Its role includes:

- fostering a culture of risk awareness and risk management;
- consideration of draft risk policies, strategies and registers;
- ensuring that risks and risk management are included in project proposals or work plans presented to it for consideration or approval; and
- ensuring that there is ownership for all significant risks by a member of CMT.

Staff and partners

10. Members of staff and the partner firms that act as appointed auditors or contractors are expected to:

    - be familiar with the OAG's policy on and approach to risk management;
    - to be risk aware in their work;
    - to take responsibility for the ownership of risks assigned to them;
    - to inform managers if they become aware that business objectives could be at risk; and
    - to take a corporate approach to risk by considering the implications for the whole organisation of individual risk management actions.

11. This risk management policy and the risk register will form part of the induction training for new staff.

RISK REGISTER

12. The OAG will maintain a corporate level risk register under the ownership of the Auditor General. The register will be updated and considered by the CMT at its meetings on a quarterly basis. Full updates will be carried out in parallel with the budgeting, operating and strategic planning cycle.

13. The risk register is intended to be a dynamic document reflecting the fact that risks may change between formal reviews. The register will be updated between reviews to reflect changes in risks as they are identified.

14. The risk register is intended to cover corporate wide risks and risks to corporate developments. Risks to individual audits, studies and projects should be recorded and reported through operational planning and monitoring processes unless they are so significant or pervasive that they pose a risk to corporate level objectives. For example, a delay to an individual audit or report would not normally appear on the corporate risk register, but delays to a whole range of audits may appear if that represents a risk to meeting corporate delivery or quality objectives.

Structure of the risk register

15. The register will group risks by category and should include the following components for each risk:

    - gross risk assessments of likelihood and impact;
    - controls/actions in place to mitigate the gross risks;
    - net risk assessments of likelihood and impact;

- further actions or monitoring required including timescales and reference to any relevant key performance indicators;
- target risk score; and
- identity of risk owner.

16. The categories the risks should be grouped under are:

- Strategic e.g. reputational, independence,
- Quality e.g. incorrect opinion, inadequate processes, systems and resources to ensure quality outcomes
- Financial e.g. inadequate resources to deliver mandate
- Operational e.g. natural disasters, IT breaches, physical access
- Our People e.g. changing legislation/government policies, maintaining sufficient staff, up to date skills; health and safety

Risk appetite, risk target, risks assessment and actions to reduce

17. Our appetite for risks will be determined for a particular risk, and a target score will then be set. Once the risk assessment process is completed, we will document the net risk assessment score. This will be compared to the target, and a determination will be made on what further actions can be taken to reduce the risk to an acceptable risk. These risk targets will be reassessed after the implementation of the necessary actions to reduce the risk and determine whether it is now at an acceptable level.

18. The likelihood and impact of each risk should be scored in accordance with Table A below.

19. Traffic lights will be used to identify the highest scoring net risk assessments, which will be those requiring the greatest Management Team attention. For net risk assessments, Table B indicates the OAG's appetite for different levels of risk.

20. Risk owners will be assigned and are required to report on how risk is being managed to the CMT. This review will occur quarterly as described in paragraph 12 above.

Table A

		LIKELIHOOD				
IMPACT	**Multiplier**	**Rare**	**Unlikely**	**Possible**	**Likely**	**Almost Certain**
Multiplier		1	2	3	4	5
Fundamental	5	5	10	15	20	25
Major	4	4	8	12	16	20
Moderate	3	3	6	9	12	15
Minor	2	2	4	6	8	10
Insignificant	1	1	2	3	4	5

Table B

Net risk assessment	Risk appetite response
20-25	Unacceptable level of risk exposure which requires immediate corrective action to be taken
11-19	Tolerable level of risk that requires constant active monitoring and action to be taken to reduce exposure
5-10	Acceptable level of risk exposure subject to regular active monitoring Measures
1-4	Acceptable level of risk exposure on the basis of normal operation of controls in place

Template risk register and example entry

21. A template for the corporate level risk register is attached.

OTHER RISK MANAGEMENT ARRANGEMENTS

22. Risk management will also be included in the project planning for major corporate projects. The nature and extent of documentation will depend on the significance of the project and the risks involved.

DISSEMINATION AND REVIEW OF THE RISK POLICY AND STRATEGY

23. This policy and strategy will be published on the OAG's website and available to all staff.

RISK REGISTER TEMPLATE

Risk Description	Gross Risk			Controls in place	Net Risk			Further action and date of implementation	Target Risk Score	Risk Owner
	Likeli hood	Impact	Total		Likeli hood	Impact	Total			