The Institute of Internal Auditors
L'Institut des auditeurs internes
Canada

# Directive on Internal Audit for Artificial Intelligence (AI)

*Issued pursuant to the Policy on Internal Audit*

This Directive supports the objectives of the Policy on Internal Audit by establishing mandatory requirements for internal audit assurance and advisory engagements respecting the governance, risk management and internal controls of artificial intelligence used by departments. It supplements, and is to be read together with, the Directive on Internal Audit, which it does not replace.

This Directive is to be read in conjunction with the Policy on Internal Audit, the Directive on Internal Audit, the Directive on Automated Decision-Making, the Policy on Service and Digital, and applicable legislation respecting privacy, security, information management, procurement and accessibility.

Internal audit engagements conducted under this Directive, whether assurance or advisory, must be performed in accordance with the International Professional Practices Framework (IPPF), including the Global Internal Audit Standards, issued by The Institute of Internal Auditors. Where any provision of these professional standards conflicts with the Policy on Internal Audit, the Directive on Internal Audit, or this Directive, the applicable Policy or Directive will prevail.

## 1. Effective date

1.1 This Directive takes effect on [Date].

## 2. Authorities

2.1 This Directive is issued pursuant to the same authorities as those indicated in section 2 of the Policy on Internal Audit.

2.2 This Directive is issued pursuant to the Directive on Internal Audit and sets out additional requirements applicable to internal audit activities involving artificial intelligence.

## 3. Definitions

3.1 In this Directive, artificial intelligence system means any system, tool or service that uses artificial intelligence to perform tasks that would otherwise require human intelligence, including:

a. generative artificial intelligence, defined as a type of AI capable of creating new and novel outputs, such as text, code, images, videos, and audio;
b. machine learning models; meaning the ability of algorithms and statistical models to learn and adapt without being explicitly programmed;
c. large language models; defined as a type of generative AI trained on vast amounts of data with many parameters that generate novel text-based responses;
d. predictive analytics tools;
e. artificial intelligence embedded within commercial, off-the-shelf or vendor-supplied software; and

f. agentic artificial intelligence solutions capable of taking autonomous or semi-autonomous action.

3.2 For greater certainty, this Directive applies to artificial intelligence systems described in section 3.1 regardless of whether they are internally developed, commercially acquired, embedded within other software, cloud-hosted, or provided as a service by a third party, so that departments do not interpret this Directive narrowly so as to exclude AI-enabled platforms.

3.3 In this Directive, assurance engagement means an internal audit engagement in which internal auditors provide an independent and objective assessment of the governance, risk management or internal controls over artificial intelligence, for which conclusions are reported to management, the deputy head and the departmental audit committee.

3.4 In this Directive, advisory engagement means an internal audit engagement in which internal auditors provide advice, insight or facilitation respecting the governance, risk management or internal controls over artificial intelligence, the nature and scope of which are agreed with management, and in which internal auditors neither provide assurance nor assume management responsibilities.

## 4. Objectives and expected results

### 4.1 Objectives

The objectives of this Directive are to:

a. extend the internal audit requirements of the Directive on Internal Audit to the governance, risk management and control of artificial intelligence;
b. support deputy heads in obtaining independent assurance and objective advice over the management of risks associated with artificial intelligence;
c. Promote responsible and secure use of artificial intelligence across government, supported by appropriate transparency, oversight, and accountability; and
d. enable internal audit to contribute, at an early stage and on a timely basis, to the design and implementation of effective governance, risk management and controls over artificial intelligence, while preserving its independence and objectivity.

### 4.2 Expected results

The expected results set out in section 3 of the Policy on Internal Audit apply to this Directive, including the provision of risk-informed, independent assurance over the governance, risk management, and internal controls associated with departmental use of artificial intelligence, and, where appropriate, objective advice that strengthens those arrangements before and after artificial intelligence systems are deployed.

## 5. Requirements

### 5.1 Deputy heads

Deputy heads are responsible for ensuring that:

a. artificial intelligence risks are incorporated into departmental governance and risk management;
b. internal audit teams have unrestricted access to the information required to assess governance and controls over artificial intelligence;
c. management action plans responding to internal audit findings on artificial intelligence are implemented in a timely manner; and
d. internal audit is informed of significant artificial intelligence initiatives at an early stage, including design, procurement and deployment, so that the Chief Audit Executive can determine whether advisory or assurance engagements are warranted.

### 5.2 Chief Audit Executives

In addition to the requirements of section 4 of the Directive on Internal Audit, Chief Audit Executives shall:

a. consider artificial intelligence risks when preparing the departmental risk-based internal audit plan, including planned assurance and advisory engagements respecting artificial intelligence;
b. periodically assess departmental governance, risk management and internal controls over artificial intelligence, in accordance with Appendix A;
c. Communicate significant audit findings, risks, and recommendations related to the governance and use of artificial intelligence to senior management and the departmental audit committee in a timely manner;
d. Monitor the implementation of management action plans arising from internal audit engagements related to artificial intelligence and, where management has not taken timely and appropriate action to address significant identified risks or recommendations, report the matter to senior management and the departmental audit committee;
e. where appropriate, provide advisory services respecting artificial intelligence, in accordance with section A.7 of Appendix A, in a manner that does not impair the independence of the internal audit function or the objectivity of internal auditors;
f. ensure that management retains responsibility for all decisions arising from advisory services, and that internal audit does not design, implement, operate or approve artificial intelligence systems or controls; and
g. inform the departmental audit committee of advisory services provided respecting artificial intelligence, including any prior advisory involvement in a system, framework or control that is subsequently the subject of an assurance engagement, and the safeguards applied.

### 5.3 Departmental Audit Committees

Departmental Audit Committees shall review the adequacy of assurance provided over significant risks, and significant audit findings, relating to artificial intelligence, and the appropriateness of advisory services provided by internal audit respecting artificial intelligence, including the balance

between assurance and advisory coverage and the safeguards applied to protect independence and objectivity, consistent with their responsibilities under the Policy on Internal Audit.

**5.4 Management**
Management remains responsible for governance, risk management and internal controls over artificial intelligence. Internal audit does not assume management's responsibilities in this regard, whether in the course of assurance or advisory engagements. Where internal audit provides advice respecting artificial intelligence, management remains responsible for deciding whether and how to act on that advice, and for all decisions respecting the design, approval, deployment, operation and retirement of artificial intelligence systems.

## 6. Roles of other government organizations

6.1 The roles and responsibilities of other government organizations with respect to the governance, oversight, security, privacy, and use of artificial intelligence continue to apply in accordance with their respective mandates. Nothing in this Directive alters those responsibilities or transfers management accountability for artificial intelligence to the chief audit executive or the internal audit function, including where internal audit has provided advice respecting artificial intelligence.

## 7. Application

7.1 This Directive applies to the organizations described in section 6 of the Policy on Internal Audit.

7.2 This Directive applies to all artificial intelligence systems used by departments, as defined in section 3, including internally developed, commercially acquired, cloud-hosted, embedded and third-party systems, throughout their lifecycle, including during planning, design and procurement, when advisory engagements may be of particular value.

## 8. References

8.1 Legislation

- Financial Administration Act

8.2 Related policy instruments

- Policy on Internal Audit
- Directive on Internal Audit
- Directive on Automated Decision-Making
- Policy on Service and Digital
- Directive on Privacy Practices
- Directive on Security Management

## 9. Enquiries

9.1 For interpretation of any aspect of this Directive, contact Treasury Board of Canada Secretariat Public Enquiries.

9.2 Individuals from a departmental internal audit group may contact the Internal Audit Sector for interpretation.

## Appendix A: Mandatory Procedures for Internal Audit Engagements Respecting Artificial Intelligence

### A.1 Effective date

A.1.1 These procedures take effect on the same date as this Directive.

### A.2 General

A.2.1 These procedures provide details of the requirements set out in section 5 of this Directive.

A.2.2 Internal audit engagements respecting artificial intelligence are carried out in accordance with the International Professional Practices Framework, as issued by The Institute of Internal Auditors, and the following mandatory procedures.

A.2.3 Sections A.3 to A.6 apply to assurance engagements and, as appropriate, to advisory engagements. Section A.7 sets out additional procedures that apply to advisory engagements. The audit considerations in section A.4 may also be used to scope advisory engagements.

### A.3 Planning

A.3.1 Chief Audit Executives should ensure that internal audit engagements respecting artificial intelligence are proportionate to risk, considering:

a. impact on Canadians;
b. financial significance;
c. sensitivity of the information involved;
d. national security and the public interest;
e. degree of automation and complexity of algorithms;
f. reliance on third-party technologies; and
g. previous audit findings or incidents involving artificial intelligence.

A.3.2 In planning engagements respecting artificial intelligence, Chief Audit Executives should also consider whether the department:

a. maintains a current inventory of artificial intelligence systems in use or under development;
b. artificial intelligence systems have a designated owner or responsible party within the organization that is ultimately responsible for the systems' actions and outcomes;
c. classifies artificial intelligence systems according to their level of risk or impact;
d. has identified high-impact artificial intelligence systems requiring enhanced oversight; and
e. has conducted impact assessments, including in accordance with the Directive on Automated Decision-Making, where applicable.

The absence of a departmental artificial intelligence inventory or risk classification is itself a relevant consideration for risk-based audit planning and may indicate where an advisory engagement could help management establish these foundations before assurance is provided.

A.3.3 In preparing the risk-based internal audit plan, Chief Audit Executives should identify where early internal audit input through advisory engagements may be of value, such as:

a. new or high-impact artificial intelligence systems in planning, design or procurement;
b. the establishment or revision of departmental artificial intelligence governance frameworks, policies, inventories or risk classification methods;
c. the development of artificial intelligence-specific contractual clauses and vendor due diligence processes including artificial intelligence enterprise agreements;
d. the enterprise-wide adoption of generative artificial intelligence tools; and
e. the maturity assessment referred to in section A.6.2.

**A.4 Audit considerations**

Internal audit engagements respecting artificial intelligence should be assessed, as applicable:

A.4.1 Governance — governance structures, roles, responsibilities, accountability and ethical oversight, including whether the department has designated an accountable executive for artificial intelligence, established an artificial intelligence governance committee or equivalent oversight body, assigned clear ownership of artificial intelligence risk and of individual models or systems, and maintains a formal inventory of artificial intelligence systems;

A.4.2 Risk management — identification, assessment, mitigation and monitoring of risks, including privacy, cybersecurity, bias, discrimination, explainability, model drift, legal compliance and operational resilience. Cybersecurity considerations should include artificial intelligence-specific threats such as prompt injection attacks, model poisoning, adversarial attacks, application programming interface security, model theft, resilience of artificial intelligence services, and monitoring for abuse of artificial intelligence systems;

A.4.3 Internal controls — controls over data quality, model development and validation, access and change management, monitoring, incident management, documentation and record keeping, including model lifecycle controls such as model approval processes, independent validation, periodic revalidation, change management for model updates, training data management, and retirement and decommissioning procedures, recognizing that many artificial intelligence failures occur after deployment due to model drift and unmanaged changes;

A.4.4 Human oversight — appropriate human review of significant decisions, retention of accountability with public officials, and escalation procedures;

A.4.5 Information management — lawful collection, accuracy, protection, retention and disposal of information used by artificial intelligence systems, including training data lineage, data quality controls, testing for bias in training data, data provenance, consent and legal basis for the use of data, and controls over cross-border transfers of data;

A.4.6 Procurement — satisfaction of procurement requirements, adequacy of contractual controls, audit rights and management of vendor risk, where artificial intelligence services are obtained from third parties, including consideration of model hosting location and data sovereignty, sub-processor transparency, vendor rights to update or retrain models without

customer approval, ownership of prompts, outputs and training data, artificial intelligence-specific contractual protections, and explainability commitments from vendors; and

A.4.7 Generative artificial intelligence controls — controls specific to generative artificial intelligence tools, including prompt management controls, protection of sensitive information entered into generative artificial intelligence tools, validation of artificial intelligence-generated outputs, risks of intellectual property violations, management of hallucination risk, human approval requirements for outputs used in decision-making, monitoring of artificial intelligence output use, and user training and acceptable use requirements.

**A.5 Reporting**

A.5.1 Internal audit assurance engagement reports respecting artificial intelligence should be finalized in accordance with section 4 of the Directive on Internal Audit and should include, as applicable, governance observations, significant risks, control deficiencies, root causes, recommendations, management responses and implementation timelines.

A.5.2 Significant issues should be communicated promptly to senior management and the departmental audit committee, including significant issues identified in the course of advisory engagement, whether or not they fall within the agreed scope of the engagement.

A.5.3 The results of advisory engagements respecting artificial intelligence should be communicated in the form agreed to with management under section A.7.2 and need not include an assurance conclusion or rating.

**A.6 Monitoring**

A.6.1 Chief Audit Executives should monitor the implementation of management action plans arising from internal audit engagements respecting artificial intelligence.

A.6.2 Because artificial intelligence risks evolve continuously and cannot be addressed through periodic audits alone, departments should periodically assess the maturity of governance and internal controls supporting artificial intelligence, and should consider ongoing monitoring of model performance, bias and accuracy, drift detection, and analysis of incident trends. Chief Audit Executives may support this maturity assessment in an advisory capacity, for example by providing a methodology or facilitating a self-assessment, provided that management retains ownership of the assessment and its results.

A.6.3 The maturity assessment referred to in A.6.2 should consider, at a minimum, the following domains:

| Domain | Example Criteria |
|---|---|
| Governance | Roles, committee oversight, accountability |
| Risk Management | AI risk assessments, impact assessments |
| Controls | Technical and operational controls |
| Data Management | Data quality, lineage, privacy |
| Third-Party Risk | Vendor oversight |
| Model Risk Management | Validation, drift monitoring |
| Audit and Assurance | Assurance and advisory coverage, independence safeguards and reporting |

This maturity assessment framework provides departments with a repeatable improvement path across governance, risk management, controls, data management, third-party risk, model risk management, and audit and assurance.

**A.7 Advisory engagements**

A.7.1 Nature and scope. Chief Audit Executives may provide advisory services respecting artificial intelligence, which may include:

a. advice on the design of artificial intelligence governance frameworks, including oversight body mandates, accountabilities, and system and model ownership;
b. design or pre-implementation reviews of controls over artificial intelligence systems, including the model lifecycle controls described in section A.4.3;
c. advice on risk and impact assessment methodologies, including algorithmic impact assessments under the Directive on Automated Decision-Making;
d. advice on artificial intelligence-specific contractual safeguards, audit rights and vendor due diligence, as described in section A.4.6;
e. facilitation of risk and control self-assessments, including the maturity assessment referred to in section A.6.2;
f. training and awareness for management and staff on artificial intelligence risks and controls; and
g. participation in artificial intelligence governance committees or equivalent oversight bodies in an advisory, non-voting capacity.

A.7.2 Agreement with management. Before an advisory engagement begins, the Chief Audit Executive and the responsible manager should agree, in writing, on its objectives, scope, respective responsibilities, deliverables, timelines and the manner in which results will be communicated.

A.7.3 Independence and objectivity safeguards. In providing advisory services respecting artificial intelligence, internal auditors shall not:

a. design, develop, implement, operate or approve artificial intelligence systems, models or controls;
b. make management decisions or accept accountability for artificial intelligence risk;
c. own or maintain the departmental artificial intelligence inventory, risk classification or any model;
d. perform the independent model validation function referred to in section A.4.3 on behalf of management; or
e. act as a voting member of an artificial intelligence governance committee or equivalent oversight body.

A.7.4 Subsequent assurance engagements. Where internal audit has provided advice respecting an artificial intelligence system, framework or control that later becomes the subject of an assurance engagement, the Chief Audit Executive should assess whether objectivity may be impaired, should consider assigning internal auditors who did not participate in the advisory engagement, and should disclose the prior advisory involvement in the engagement report and to the departmental audit committee.

A.7.5 Balance with assurance coverage. Chief Audit Executives should ensure that advisory services respecting artificial intelligence do not displace adequate assurance coverage of significant artificial intelligence risks.

A.7.6 Competencies. Chief Audit Executives should ensure that internal auditors performing advisory engagements respecting artificial intelligence collectively possess the necessary knowledge, skills and competencies, and may obtain the assistance of qualified external experts where required, consistent with the Global Internal Audit Standards.

A.7.7 Documentation. Advisory engagements respecting artificial intelligence should be documented, including the agreement referred to in section A.7.2, the work performed, the advice provided and the safeguards applied under sections A.7.3 and A.7.4.

For any questions regarding this proposal or for a briefing on the internal audit profession, please contact Ryan Singh at Ryan.Singh@TheIIA.org.