



Canadian Public Accountability Board
Conseil canadien sur la reddition de comptes

CPAB audit risk alert – Use of artificial intelligence applications in the audit

Background

Over the past year there has been a significant advancement in the general availability of applications incorporating artificial intelligence (AI), many of which could be used by auditors and management of Canadian reporting issuers. Examples include:

- Applications used by auditors that analyze populations to identify unusual trends and areas of potential audit interest.
- Generative artificial intelligence applications (prominent examples include Chat GPT, Bing Chat, Bard and DALL-E) used by both auditors and management teams to perform research and generate reports, presentations, images or other media.

While the potential of these technological advancements to improve the effectiveness and efficiency of the audit is significant, it also creates risks that must be effectively managed. Before audit firms and audit engagement teams use these applications, it is essential that audit firms adopt appropriate safeguards to manage any risks to audit quality in the same fashion that these risks are managed with automated tools and techniques currently used in audits. The complexity of some AI platforms may require audit firms to use appropriate AI experts to perform this evaluation.

An audit firm may need to prohibit the use of these applications until the firm has obtained a sufficient understanding and tested the operation and trustworthiness of the IT application.

What should audit firms consider prior to using these tools?

The management of audit quality risks from IT applications should be built into each audit firm's system of quality management.¹

A firm may find it necessary to consider the following matters in obtaining, developing, implementing and maintaining an IT application:

- The completeness and appropriateness of data inputs.
- Confidentiality of data.
- Whether the IT application operates as intended.
- The effectiveness of the IT application's outputs.
- The appropriateness of general IT controls to support the continuous operation of the IT application.
- The sufficiency of specialized skills within the audit engagement team to effectively utilize the IT application, including the training of individuals using the IT application.

¹ CSQM 1, paragraph 32(f)

- Established procedures that set out how the IT application operates.²

Practical risk considerations include:

- **Reliability and explainability** – AI applications often employ complex algorithms to generate outputs which may lack transparency and understandability. Audit firms or engagement teams should evaluate the reliability of the output and their ability to explain how the tool reached its conclusion and/or generated its output. This may include obtaining sufficient understanding of the underlying algorithm and the data that was used to train the application.
- **Confidentiality** – The data collected by AI applications may not remain confidential. Audit firms or engagement teams should consider whether information they input into an application will remain confidential in accordance with professional obligations.

In order to mitigate these risks, the following safeguards may be necessary:

- Instructing engagement teams not to use AI applications until the firm has obtained a sufficient understanding and properly tested the operation of the IT application.
- Developing a policy on the use of AI tools within the firm and on audits and providing staff training on the risks and appropriate use of these tools.
- Establishing a protocol to monitor the use of AI tools within the firm and on audits, including whether the applications are being used as intended and achieving the desired audit quality impact.

Other considerations – impact on the quality of audit evidence

Auditors also need to be aware of the risk that information provided to them by management teams is created using AI applications such as generative IT tools. As with all other information provided by an entity, auditors should apply professional skepticism including steps to verify that the information provided is complete and accurate and can be used as appropriate audit evidence.

We want to hear from you

An objective of this publication is to serve as the foundation for ongoing discussions with audit firms, auditing standard setters and other regulators. We would like to hear from you. Please send your comments or questions to thoughtleadership@cpab-ccrc.ca.

² CSQM 1, paragraph A100.