Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Guide to Peer Review of Automated Decision Systems

Published: 2025-01-06

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT48-52/2025E-PDF
ISBN: 978-0-660-75244-0

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Guide sur l’examen par les pairs des systèmes décisionnels automatisés

Guide to Peer Review of Automated Decision Systems

On this page

Importance of peer review

The *Directive on Automated Decision-Making* is a policy instrument that sets requirements for federal departments to ensure that the use of artificial intelligence (AI) or other automated systems in administrative decision-making is compatible with the core principles of administrative law such as transparency, accountability, legality and procedural fairness. Section 6 of the directive lists these requirements, one of which is to complete an Algorithmic Impact Assessment (AIA) that will determine the scaled requirements of the directive based on the calculated impact level of an automation project. Projects assigned an impact level of 2 or higher are subject to the peer review requirement (subsection 6.3.5) that mandates publication of a complete review or plain language summary prior to the system's production.

Peer review is a quality assurance mechanism in which the project is subject to scrutiny by experts in the relevant domain. In the context of the directive, it involves an assessment of the AIA and supporting documentation to validate content integrity, technical soundness and ethical considerations. The completion and publication of a peer review can help departments:

- have confidence in the quality of their automated system
- ensure effective compliance with the directive
- foster greater transparency

Purpose

This document supports federal departments commissioning a peer review and individuals undertaking the review. It defines a process, proposes roles and responsibilities, and identifies best practices to improve the consistency and robustness of reviews. The guide can also serve as a reference for other bodies undertaking similar reviews of AI systems. The *Peer Review for Automated Decision-Making Tools Under Canada's Directive on Automated Decision-Making* (Bronson and Millar, 2020) report was a key source that helped inform the development of this guidance.

The peer review process

▼ In this section

Prepare for peer review

Confirm need for peer review

To determine applicability of the peer review requirement, departments should first confirm that their project is within scope of the directive. The directive applies to any system, tool or statistical model used to make or support an administrative decision or related assessment about a client. Refer to the *Guide on the Scope of the Directive on Automated Decision-Making* for more information on the key elements of scope that departments should consider and examples of systems that are in and out of scope.

Projects within scope of the directive must complete the AIA (section 6.1), an online questionnaire designed to help departments better understand and manage the risks associated with automated decision systems. The AIA is composed of weighted questions that assess factors such as a system's design, algorithm, decision type, impact and data. Responses to the questions contribute to a score that determines the impact level assigned to a project. The impact level ranges from 1 (little impact) to 4 (very high impact). Projects assigned an impact level of 2, 3 or 4 must undergo peer review.

Identify suitable reviewers

Departments commissioning a review should contact and select potential reviewers. Appendix C of the directive identifies requirements that are proportionate to the impact level. At least one expert must be consulted for impact levels 2 and 3. As a project's impact level increases, it is expected that departments consult a greater number of experts (that is, at least two for impact level 4). The inclusion of multiple experts at all levels is strongly recommended to ensure diverse views and representation of the skills and knowledge needed to accurately assess both technical and ethical issues.

Areas of expertise

The areas of expertise needed may vary according to the project. Reviewers should be qualified subject matter experts with specialized knowledge and experience relevant to the project in areas, including both of the following:

- technical: artificial intelligence, machine learning, data science, statistics, computer science, systems engineering or other related fields
- ethical: ethics, privacy, public policy, diversity and inclusion, human-centred design or other relevant areas

Qualifications and experience

To be considered a qualified expert, reviewers must have sufficient depth and breadth of expertise obtained from at least five years of work experience. Examples of relevant work experience could include the following:

- conducting research and analysis of sociological impacts of projects, programs or policies, for example, by using a diversity, human rights or Gender-based Analysis Plus (GBA Plus) framework
- analyzing datasets to uncover insights, build models, test for biases and inform decision-making
- designing, developing and implementing automated decision systems or AI solutions
- evaluating systems across life cycles from a socio-technical perspective

A combination of education and experience may serve as an alternative to work experience at the discretion of the department.

Experts must also hold or be able to obtain the appropriate security clearance prior to conducting the review.

Experts

Experts should be aligned with the options in Appendix C of the directive:

- experts from a federal, provincial or municipal government institution

- faculty members of a post-secondary institution
- researchers from civil society organizations (for example, non-governmental organizations, advocacy groups, labour unions, professional associations)
- third-party vendors or individuals from other external organizations
- members of a data and automation advisory board specified by the Treasury Board of Canada Secretariat (TBS)

Where possible, it is recommended that stakeholders from impacted groups are included in consultations on peer review across impact levels 2 to 4. In addition, consider intersecting identity factors such as gender, race and ethnicity to promote diversity and inclusion when selecting reviewers.

Departments opting to have a data and automation advisory board conduct the review should contact TBS (ai-ia@tbs-sct.gc.ca) and provide the completed AIA, information on the system, timelines and required security classifications.

Manage conflict of interest

Reviewers are expected to disclose any conflicts of interest that could compromise the impartiality of a review. For example, any of the following situations could be considered a real, apparent or potential conflict of interest:

- previous or current involvement in the system design or implementation
- an institutional affiliation or other professional or personal relationship
- remuneration in exchange for the review

The department is responsible for vetting appropriate experts and ensuring that any conflicts of interest disclosed have been assessed and mitigated prior to entering into an agreement. This includes ensuring that the documented agreement with the reviewer includes a conflict of interest declaration.

As well, all federal public servants must comply with the *Directive on Conflict of Interest* and the *Values and Ethics Code for the Public Sector* for the entirety of the review process. If the department contracts a reviewer from outside the federal government, the reviewer should abide by the requirements to disclose conflicts of interest as described in the *Code of Conduct for Procurement*. If a conflict of interest cannot be mitigated, the department and reviewer should not enter into an agreement. If an agreement already exists, the reviewer should recuse themselves from the review and the department should terminate the review agreement.

To avoid conflict of interest, consider the following best practices:

- Select experts that are external to your department. If commissioning expertise within the public service, ensure that reviewers are not in a closely affiliated business line and have

not been involved in the project.
- Be mindful of reciprocal reviews. For example, departments reviewing each other's work could be perceived as a biased agreement that undermines the objectivity and integrity of peer review.
- If applicable, any remuneration provided should be fair for all external reviewers, clearly documented and received by the institution where possible.
- Reach out to your departmental values and ethics team for advice on specific cases. Encourage the reviewer to connect with the values and ethics team in their organization.

Establish clear timelines

Early engagement is encouraged, as the time needed to complete a review will vary depending on the system's complexity, impact level, number of reviewers and security clearance required. The department should ensure sufficient time for review (for example, one to three months) in the project plan. The review should be initiated early enough so that identified issues can be addressed but far enough into the project life cycle that sufficient information is available for assessment against the actual system just prior to production. A review should occur after privacy assessments (such as a Privacy Impact Assessment or privacy protocol) and after the AIA and security assessments have been completed or are underway. Projects that follow an agile development process should aim to have the review completed prior to initial software production.

Clarify roles and responsibilities

The department should clearly define respective responsibilities in a documented agreement with the reviewer. Refer to the Statement of Work template for an example agreement.

Department

The federal department planning to use an automated decision system:

Project documentation

- Completes the AIA and assembles supporting documentation, including ensuring that documentation is available from third parties for systems developed externally (refer to the suggested documentation list)
- Ensures that necessary funds are available and that agreements involving remuneration are in accordance with federal policies
- Develops a statement of work that sets out key elements such as purpose, scope, timelines, deliverables and security clearance required

Engagement and transparency

- Contacts potential reviewers and selects the most suitable among them
- Proactively identifies any potential concerns or areas where there may be weaknesses (for example, incomplete or biased training data)
- Fosters open communication in which reviewers may engage with the project team and developers throughout the process
- Discloses and describes any uses of generative AI to support system design and development

Publication and reporting

- Provides and considers publication of a response to the final report that specifies changes and commitments made or provides a rationale for not accepting recommendations
- Coordinates translation and approvals to publish the review
- Ensures that all published content is available in English and French
- Produces a summary of the final report in consultation with the reviewer if opting to not publish the complete review

Reviewer

The individual undertaking the review with expertise in the relevant context:

Expertise and conflict management

- Confirms having the expertise and availability needed to conduct the review and participate in follow-up discussions
- Discloses any possible conflicts of interest, including financial, personal, professional or institutional relationships with the department

Review process and reporting

- Critically assesses the automated decision system across areas, including but not limited to the Complete the Review Checklist. This includes validating the completion and quality of AIA responses and assessing the supporting documentation without necessarily replicating the outputs
- Provides regular updates
- Maintains confidentiality of the peer review process and related information in compliance with applicable policies and laws
- Prepares a written report, ensuring that comments are fair and recommendations focus on specific actions and areas for improvement. If a project involves multiple reviewers, each one is contributing to their area of expertise to develop a single consolidated report

- Discloses and describes any uses of generative AI to support the review. Refer to the *Guide on the Use of Generative Artificial Intelligence* for best practices and documentation requirements

Suggested documentation for peer review of automated decision systems

The following should be captured in the documentation provided by the department to the reviewer. In many cases, a well completed AIA will include much of the information below.

Roles and responsibilities

- Roles and responsibilities for the design, development, deployment, use and monitoring of the system (for example, policy and legal authorities, confirmation of approvals)
- Training and system instructions or procedures provided to employees and information on potential impacts to staff

System functionality and documentation

- Description of system functionality (for example, reasons for automation, anticipated benefits to the client and organization, points of human intervention during the decision-making process, limitations of use)
- Information about and access to the model (for example, model type, other models considered or tested, hyperparameters chosen and approach to tuning and optimization, model performance and metrics, implementation readiness, intellectual property or licence restrictions)
- Audit trails and information on the processes that support their use
- System documentation such as requirements, data model, source code and architecture design

Data management and privacy

- Information on the data (for example, data provenance, data-sharing agreements, approach to assess and resolve data quality issues and impacts of any remaining issues on the system, data governance measures for input and generated data)
- Access to data: When data is required for the review, if data has been manipulated (for example, de-identified); the department in collaboration with the reviewer should determine whether this would allow for a sufficient review (more information on de-identification is available in Privacy Implementation Notice 2023-01: De-identification)

- Information on privacy measures undertaken (for example, privacy-enhancing technologies, completed privacy impact assessment)

Fairness, transparency and impact analysis

- Fairness and transparency assessment
- Analysis of the impacts on clients including evidence of bias testing of the data and model and mitigation measures, recourse options and a completed GBA Plus
- Evidence of transparency measures such as notice, explanations and any supporting information, including release of source code and reporting information
- Stakeholders consulted and summary of feedback received (for example, a "What We Heard" report)

Risk management and security

- Risk mitigation strategies
- Interim or final authorization to operate
- Supply chain security risk assessment report from the Canadian Centre for Cyber Security for all software and applications being developed or procured from outside the Government of Canada
- Business and information technology (IT) continuity strategies and contingency plans for impact levels 3 and 4
- Procurement details for systems developed by a third party

Complete the peer review

Using the Complete the Review Checklist and documentation provided by the department, reviewers should assess the following areas. Given the broad areas of expertise required, multiple reviewers working together to produce a single report is recommended to ensure an adequate and holistic review. Reviewers are also encouraged to provide input on technical and ethical components not captured below.

Accuracy and completeness of AIA

The AIA is a key document that should be carefully reviewed. As a first step, reviewers should validate the responses against available information to confirm the impact level. Reviewers should also identify any discrepancies in responses that would warrant the AIA to be updated. If there is a need for an updated AIA, the reviewer should not proceed further until the discrepancies have been discussed and addressed. This is essential, as the impact level informs the applicable requirements under the directive.

Readiness to comply with the directive

The peer reviewer should be familiar with the *Directive on Automated Decision-Making* and use the evidence provided to identify any potential gaps in compliance. In addition to verifying the completion of an AIA (subsection 6.1), the reviewer should validate that steps have been taken to meet requirements related to transparency (subsection 6.2), quality assurance (subsection 6.3), recourse (subsection 6.4) and reporting (subsection 6.5).

Data quality

Good data quality is a necessary foundation to build high-quality systems. The peer reviewer should examine the processes that occurred and are in place to ensure that data quality is sufficient. This includes planning and decisions on data collection and use, as well as ensuring that data governance is in place for any data used or generated by the system.

Fairness

Systems have the potential to produce inaccurate, biased or inconsistent outputs that could result in unfair outcomes. For example, biases or a lack of representation in the training data can be reflected in the outputs of the system and lead to amplification of those biases. As well, fairness captures risks related to procedural fairness where departments are obligated to provide clients with a meaningful explanation of how and why a decision was made, along with recourse options in instances where a decision results in the denial of a service or benefit.

Privacy

Systems often rely on vast amounts of data and may be vulnerable to privacy breaches. When that data constitutes personal information, it must be managed in accordance with the *Privacy Act* and related policy instruments. If there is a serious possibility that an individual could be identified, alone or in combination with other information, this information may constitute personal information. The reviewer should confirm that the department has verified that it has the legal authority to collect personal information and that the collection is limited to what is directly related to operating a program or activity of the department. If personal information is being handled, the reviewer should validate that departmental privacy officials have been consulted. The privacy risks will vary based on the amount and type of personal information involved and how the system uses personal information to inform a decision. Refer to the *Privacy Act* and related policy instruments, including the *Digital Privacy Playbook* for more information on privacy considerations.

Security

The integration of security considerations from the onset and throughout a system's life cycle is critical to protect sensitive information, build user trust and ensure business continuity. The reviewer should ensure that effective security safeguards have been implemented to ensure the protection of confidentiality, integrity and availability throughout the system life cycle. This includes verifying that a security assessment is complete and an authority to operate has been obtained. As well, the reviewer should confirm that the department has obtained a Supply Chain Security Risk Assessment report from the Canadian Centre for Cyber Security and developed a related risk mitigation strategy. More information on security controls can be found in:

- Appendix B: Mandatory Procedures for Information Technology Security Control of the *Directive on Security Management*
- Protecting Your Organization From Software Supply Chain Threats (ITSM.10.071)
- *IT Security Risk Management: A Lifecycle Approach (ITSG-33)*

Model development

The decisions made during model development impact the operation and outputs of the system. Models can also perform differently over time and across different client groups. Peer reviewers should have access to the model where possible and review the documentation to ensure that the model is appropriate for its intended use.

Risk management

A robust risk management practice is essential to ensure that risks are identified and managed as they arise. Risks can occur pre-deployment as well as during system operation. The AIA helps identify risks, however, an ongoing approach to risk management that is integrated with the departmental risk management approach and based on recognized federal or international risk management frameworks is also needed. Reviewers should confirm that risks have been considered and processes for continuous risk management are in place.

Governance

Clear roles and responsibilities for the system and its data and outputs are important to ensure accountability for the decisions that the system makes or supports. Reviewers should validate that departments have established appropriate governance measures throughout the system life cycle.

Operational readiness

The system should be fully equipped to perform its intended functions effectively and reliably in a real-world operational context. Evaluating operational readiness involves reviewing evidence of testing and verification to ensure functionality, robustness and scalability.

Change management

Successful implementation of a system is enabled by effective communication and change management practices. Reviewers should consider the department's approaches to stakeholder engagement, cultural integration and employee training.

Final report

For impact levels 2 to 3, a single report is required. If multiple reviewers are involved, the department should assign responsibility to consolidate the different areas of assessment to a single reviewer. Impact level 4 requires multiple experts to produce at least 2 independent reports.

A peer review report template is available for reviewers. Even if the template is not used, the final report should include:

- the date of review, model version, reviewer name(s) and affiliation(s)
- an executive summary, background and methodology
- findings, including:
    - accuracy and completeness of the AIA: a statement validating the assigned impact level and confirmation that the AIA was completed accurately or that there are no outstanding discrepancies
    - major issues: significant concerns regarding the validity and quality of the project; often requires substantial changes to be made before the system can launch
    - minor issues: relatively less critical concerns that don't undermine the overall quality of the system; for example, best practices that could be undertaken to supplement the project, including use of different metrics or testing as well as additional clarifications to improve writing flow and data presentation in documents to be published
- recommendations: areas and specific actions for improvement
- a conclusion
- an annex: references and supplementary materials used to support the review, including the completed checklist

Publish the peer review

The project lead in the department develops a response that includes corrective actions and commitments to the peer review findings and recommendations. The final report and response are presented to the Assistant Deputy Minister responsible for the program using the system for consideration in advance of proceeding to system launch. The department then coordinates publication of the peer review report in both official languages on the Open Government Portal prior to the system's production. Departments are also encouraged to publish the departmental response to the review. In cases where there are limitations on full disclosure due to security, intellectual property or privacy considerations, departments can opt to publish a plain language summary of the report instead, with clear justification provided.

Contact us

Please contact the TBS Responsible Data and AI team (ai-ia@tbs-sct.gc.ca) for any questions.

Related links

- Peer Review Report Template
- Complete the Review Checklist
- Statement of Work Template

Date modified:
2025-01-07