

Online Supplement for Developing an Artificial Intelligence Ethics Governance Checklist for the Legal Community

PART A: SEMI-STRUCTURED INTERVIEW GUIDE

Introduction

- *Thank you for taking the time to speak with me today. My name is Stephanie Kelley and I am a professor of management science, specializing in artificial intelligence ethics at the Sobey School of Business at Saint Mary's University.*
- *I am working on a joint research partnership with Stewart McKelvey to help lawyers in Canada responsibly implement AI to obtain its productivity and economic benefits, whilst preventing unethical AI outcomes from occurring from the technology's use.*
- *I'm joined today by my research assistant*
- *Note that for today's interview there are no right or wrong answers to the questions. What is most helpful for our research is that you feel comfortable sharing your thoughts and feelings as openly as possible. If any questions that I'm asking aren't clear to you, or you think there's another question or topic that we should talk about, please let me know. You can skip any questions you aren't comfortable answering, with no consequences for skipping them. Also feel free to take your time and pause to think about your answers.*
 - *Does that all make sense, sound good?*
- *Just to confirm, all of your responses will be kept anonymous and not associated with your name in any way when our research is shared.*
 - *With that said, noting your preferences on the informed consent form I had you fill out you are okay with audio & video recording? (or just audio, or no recording depending on what they said on their informed consent form)*
- *Great. Thank you. Let's get started.*

Interviewee Role

- Could you briefly describe what you do in the organization, particularly with respect to artificial intelligence?

Use of AI in law today

- How is AI being used in your law firm today?
- Have you had any experience working with clients using AI and was this different from the applications of AI at the firm?

Development of AI systems

- Do you have an in-house AI development team? Or do you currently use vendors? Or a combination of both?
- Can you walk me through the development process of a typical AI project in the organization.
- What about other technology projects – is there a typical development process that they follow?
- Is there any kind of approval process?
- What about monitoring?

Risks of using AI in law

- *Now I'd like to ask you some questions about the potential risks of using AI in law*
- What do you see as the risks associated with these uses of AI?
 - Probe: e.g., privacy, equity, transparency, environment, accountability, responsibility, fairness, autonomy.
 - Probe: make sure they cover both current applications and future applications that they have mentioned
 - Probe: make sure it's not just about one type of AI (for instance, generative AI issues have been highlighted frequently in the media, but they aren't the only tool being used).

Governance Tools in Place

- Are there specific assessments that other technology projects go through?
 - Probe: privacy? Cybersecurity? General risk? Other?
- Have you used a checklist or framework to help mitigate risks for any projects in the past?
 - If yes, what was it.
 - What were the challenges of this? Benefits?
- What kinds of governance tools are in place to help prevent these risks of unethical AI from occurring?
 - Probe: Follow-up as needed to get sufficient detail about each, at least the key names of the tools and basic idea.
- Outside of the realm of AI – are there other governance tools the firm uses?
 - Probe: checklists, software, boards, standards operating procedures (SOPs), trainings, codes, audits...
- What about governance tools that you might have seen at your clients that you aren't using at the firm? Could be specific to AI, or more likely for other risks that are non-AI related?
 - Probe: start by getting them to think about a recent client working with AI
 - Probe: get them to think about other clients not working with AI in highly regulated environments – financial services, healthcare, biotech, pharmaceuticals, etc.

Gaps in Governance

- Based on the risks that we discussed at the beginning of the interview, and the governance tools that are in place today (or under development) – what do you think the gaps are?
 - Probe: Another way to look at this is what do you feel needs to be implemented to help reduce the risks of unethical AI
- Generally, do you have thoughts on how legal firms in general can work to reduce the risk of unethical AI?

Conclusion

- Is there anything else that we didn't cover you think would be important or interesting for us to know?
- *Thank you very much for your time. We're really grateful for your contribution to this research. For your information, our plan is to share the final results of our research with you down the road, so that it can hopefully assist you in your future work.*

- *Please do not hesitate to contact me if you have any further thoughts, questions, or concerns about your contribution or comments.*

PART B: THE CODEBOOK

Note that the codes that were inductively developed are identified by a * otherwise, codes were deductively developed from the literature review discussed per Phase 1 of the methodology. Code categories are denoted in grey, with individual codes in white.

Code	Definition
Meta-data	Meta-data should be coded only a single time for each document, ideally using the introductory meta-data table
Meta-data: Interviewee	Refers to whether review/auditing is performed by individuals within an organization about their own organization (e.g., company AI ethics leads)
Meta-data- Interviewee role	Refers to general role/job position of the interviewee, e.g., auditor, executive, legal. Can be described qualitatively initially and briefly
Ethics Risks	Categories of ethical risks of AI.
Ethics Risks: Human oversight	Having AI systems that are designed and developed in such a way as to enable people managing the operations of the system to exercise meaningful oversight over these systems. This includes ensuring that AI systems are interpretable to an appropriate to the legal context ¹ .
Ethics Risks: Transparency	Providing clients with appropriate information about how AI systems are being used within the law firm. The information provided should be sufficient to allow the stakeholders to understand the capabilities, limitations, and potential impacts of the systems ¹ .
Ethics Risks: Fairness & Equity	Ensuring that AI systems used within the law firm are developed an awareness of the potential for discriminatory outcomes. Appropriate actions must be taken to mitigate discriminatory outcomes for individuals and groups ¹ .
Ethics Risks: Accountability	Having governance mechanisms in place are to ensure compliance with all legal obligations of AI systems in the context in which they will be used. This includes the proactive documentation of policies, processes, and measures implemented ¹ .
Ethics Risks: Safety	Ensuring that AI systems used are proactively assessed to identify harms, including those from foreseeable misuse. Measures must be taken to mitigate the risk of harm ¹ .
Ethics Risks: Validity & robustness	Having an AI system that performs consistently with intended legal and ethical objectives ¹ .

¹ High-Level Expert Group on AI. (2020). *Assessment list for trustworthy artificial intelligence (ALTAI): For self-assessment*. European Commission. https://ec.europa.eu/newsroom/dac/document.cfm?doc_id=68342

Ethics Risks: Privacy & Data Governance	Having an AI system that is stable and resilient in a variety of circumstances ¹ . This ethics risk includes the risk of client information being breached and general IT risks.
Ethics Risks: Environmental and Societal well-being	The concern that inappropriate implementation of technology might have the potential to disrupt the fabric of society. There is a recognition that there is a balance to be struck between benefiting all human beings now, as well as future generations. Again, the flourishing of democracy is seen as a concern, and especially the plurality of values, their employment, and life choices of individuals ¹ .
Ethics Risks: Autonomy*	Not having the capacity to make an informed, uncoerced decision.
Ethics Risks: External Other*	Involve other factors outside of the organization that do not fall under other ethics risks.
Ethics Risks: Internal Other*	Involve other factors within the direct control of the company that do not fall under other ethics risks.
Issues*	Involve factors/challenges that are not related directly to ethics.
Issues: Compliance with Regulations*	Challenges that arise from abiding to laws and regulatory frameworks that regulate the use of AI technologies.
Issues: Third-party Vendors*	Challenges arise due to working with third party vendors that provide goods and services to the firm.
Risks	The potential for loss, harm, or adverse outcomes arising from uncertainties of technological, human, regulatory, or other origins which may impact an organization.
Risks: Security assessment	The process of evaluating the security of an organization's IT systems, applications, and policies.
Risks: Dependence on AI tools	The risk of becoming too dependent on AI tools. certain things.
Risks: Outperformance of AI*	The risk of AI outperforming lawyers in their existing job tasks.
Risks: Billable Hours*	The risk of AI changing the billable hour structure of the law firm or law industry overall. Some employees are concerned about the impact on the billable hour.
Risks: Compliance risk*	Refers to an individual or entity within the organization who complies with regulations, standards, laws, and rules. They are involved in risk management and mitigating compliance risks to ensure that the firm complies with the legal requirements.
Risks: Human error*	An error of a human using an AI system.
Risks: Hesitation to use technology*	Hesitation in using AI technology due to any variety of reasons.
Risks: Employees going rogue*	Employees independently acting against the firm's AI policies and interests.
Risks: Other*	It refers to other risks that do not fall into the above risk categories.
Policy	A structured set of principles, guidelines, or rules established to govern decision-making, ensure compliance, manage risks, and/or standardize practices across an organization.
Policy: Ethical Standards	Set of guidelines and principles that an organization has set to ensure that decisions are made with fairness, openness, integrity and honesty.
Policy: Data security	Practice of protecting digital information from unauthorized access, corruption or theft throughout its entire lifecycle.

Policy: Risk assessment	Process of a thorough look at your workplace to identify certain things, situations, processes, etc. that may cause harm, particularly to people.
Policy: IT policies	Process of establishing guidelines for the use of information technology within an organization.
Policy: Authorized AI tools*	Discussion of the firm's policy where certain AI tools are authorized for use.
Policy: Need for AI Policy*	Participants explicitly discussed the need for AI policy (at any level – department, organization, provincial, federal, etc.)
Policy: Adaptation of existing processes*	Importance of adapting already existing policies when considering a new AI policy.
Policy: AIDA principles*	Discussion of the forthcoming Artificial Intelligence and Data Act (AIDA) in Canada, and alignment with the policy.
Policy: Other Checklists*	Talks about other checklists used in their legal practice.
Policy: Code of Professional Conduct*	Spoke about other professional codes of conduct.
Teams	A group of individuals organized to collaborate on specific tasks, projects, or objectives.
Teams: AI Task Force	A team that has been put together to assess about AI and its development and ethical use of AI technology.
Teams: Team Meeting	A scheduled conversation where employees discuss about a particular topic (for e.g., AI).
Assessments	Systematic evaluations that are used to analyze risk, compliance, and performance, often used to aid decision-making and risk management.
Assessments: Privacy Impact Assessment	A privacy impact assessment (PIA) is an analysis of how personally identifiable information (PII) is handled to ensure compliance with appropriate regulations, determine the privacy risks associated with information systems or activities, and evaluate ways to reduce the privacy risks.
Assessment: Security assessment*	It is a process of evaluating the security of an organization's IT systems, applications, and policies.
Assessment: Contractual assessment*	It is an important tool for managing risk, ensuring that parties can enter contracts more confidently and reducing the likelihood of disputes or other negative outcomes.
Assessments: Technology assessment*	Technology assessment is the practical process of determining the value of a new or emerging technology in and of itself or against existing or competing technologies, using safety, efficacy, effectiveness, outcome, risk management, strategic, financial, and competitive criteria.
Assessments: Data security assessment*	The process of evaluating the potential risks associated with an organization's data assets.
Assessments: Technical systems used for assessment*	Technical systems that aid or could aid with any form of assessments.
Assessments: EDI assessment*	The process of requesting to understand how equity, diversity, and inclusion are integrated into a third-party vendor's product or service.
Assessments: Individual assessments*	Every lawyer or staff member's performance, abilities, and contributions are assessed individually in a law firm, and the results

	serve as a framework for decisions about promotions, compensation changes, and professional growth.
Assessments: Needs assessment*	A needs assessment helps you determine what needs to be accomplished to reach your project goals.
Assessments: Risks assessment*	The overall process or method used identify hazards and risk factors that have the potential to cause harm (hazard identification). Analyze and evaluate the risk associated with that hazard (risk analysis, and risk evaluation).
Assessments: Technology assessment*	Technology Assessment is the process of evaluating technology development, analyzing the actors involved, examining social impacts, and identifying policy options to address those impacts. (The IT team uses the technology assessment).
Assessments: Time assessment*	In general, time assessment refers to the process of estimating how long a work, project, or activity will take to finish. In addition, what would continuous compliance look like from a timing perspective.
Assessments: Other*	Other aspects of assessments that did not fall under the above categories.
Stakeholders	Stakeholders encompass all organizations and individuals involved in, or affected by, AI systems, directly or indirectly.
Stakeholders: Corporate lawyers	Refers to a corporate lawyer who advises clients of their rights, responsibilities and duties under the law.
Stakeholders: AI Task Force	It is a team that the firm has been put together to assess about AI and its development and ethical use of AI technology. The team would consist of IT team, corporate lawyers, compliance risk lawyer, vendors and so on.
Stakeholders: Paralegals	A paralegal is a legal professional who works under the supervision of a lawyer and performs tasks such as legal research, drafting legal documents, and assisting with client communication.
Stakeholder- IT Team	It is a team that provides technical assistance across the organization.
Stakeholder- Vendors	Vendors are known as suppliers that sells goods or services.
Stakeholders: Chief Strategy Innovation Officer*	They are responsible for formalizing the company's strategic-planning processes, and leading the development of the strategies.
Stakeholders: Director of Risk*	They are concerned with risks that could affect the organization's long-term goals and strategic objectives.
Stakeholders: Privacy Officer*	Implementing and maintaining a privacy policy. Managing privacy training. Responding to requests for access to and correction of personal information.
Stakeholders: Administrative team*	Administrative team is responsible for managing multiple tasks and deadlines simultaneously. There are some ESG initiatives that the administrative team pursues- It definitely has a lengthy list.
Stakeholders: Data repository owner*	A data repository owner is a person or group in charge of maintaining and supervising a data repository and making sure that the information kept there is correct, secure, and available to authorized users.
Stakeholders: Director of IT*	The individual who is in charge of the information technology team.
Stakeholders: Practice innovation*	The individuals responsible for driving innovation within the legal practice at a firm.

Stakeholders: Knowledge management team	They are the one who ensures employees and customers can access valuable information.
Stakeholders: Project Managers	The individuals responsible for planning, executing, and overseeing projects to ensure they are completed on time, within scope, and on budget.
Stakeholders: Risk team*	The risk team helps in identifying, measuring and treating property, liability, income, and personnel exposures to loss.
Stakeholders: Other*	Other stakeholders are considered as other stakeholders encompass all organizations and individuals involved in, or affected by, AI systems, directly or indirectly, that do not fit in the above categories.
Onboarding process	The process used by the organization to integrate an organization or person.
Onboarding process: procedure details*	Specific details related to the process of integrating new technology into the firm.
Onboarding process: Data Security*	Within the onboarding process, the specific onboarding procedures relevant to data security.
Onboarding process: Client agreements*	Within the onboarding process, the specific onboarding procedures relevant to client agreements.
Onboarding process: Firm contract*	Within the onboarding process, the specific onboarding procedures relevant to firm contracts.

Checklist to Reduce Unethical Applications of Artificial Intelligence (AI) in Law

AI System under review:	
Individual, internal Organization, and/or Department primarily responsible for the AI System:	
Working group, AI Actors, and/or Stakeholders that contributed to this checklist review:	
Checklist last edited on (date):	

Document Map

- [Introduction](#)
- [Definitions](#)
- [Guiding Principles for the Firm’s use of AI Systems](#)
- [Instructions](#)
- [Checklist](#)

Introduction

This AI Ethics checklist (the “**Checklist**”) serves as a guiding framework for the Firm to assess and address potential ethical considerations when implementing an AI-enabled tool or process.

The Checklist is designed to be adaptable, allowing the Firm to tailor its use based on the Firm’s unique culture, risk tolerance, client base, and specific operational context, as well as the details of the AI System under review. Different AI Systems will require different levels of scrutiny, depending on their use of confidential and/or client information. The Checklist is a component of a comprehensive AI evaluation and management strategy, complementing—rather than replacing—essential organizational, technical, privacy, data security, reputational, and legal assessments.

Definitions

AI System	An AI System is a machine-based technology that generates outputs, such as predictions, content, recommendations, or decisions that can influence physical or virtual environments, based on a set of inputs, for explicit or implicit objectives. AI Systems vary in their levels of autonomy, adaptiveness, and the ways they utilize inputs.
AI System designer	The term “designer” is used in this Checklist to refer to the provider of the AI System who can make changes to the AI System’s fundamental learning patterns, core processes, functionality, etc. Examples of designers include external vendors of AI Systems to the Firm and the Firm’s internal data scientist teams, where applicable.
AI System Lifecycle	An AI System Lifecycle is the process by which an AI System is created and implemented in a business or other environment. A Lifecycle involves several phases that can include planning and design; data collection and processing; model building and/or adaptation to specific tasks; testing; evaluation, verification and validation; deployment; operation and monitoring; and retirement/decommission.
AI Actors	AI Actors are those who play an active role in the AI System Lifecycle, including organizations and individuals that deploy or operate AI.
Stakeholders	Stakeholders are all organizations and individuals involved in or affected by the AI System, directly or indirectly. AI Actors are a subset of Stakeholders, as are individuals whose data is being used in the AI System (e.g., clients of the Firm).
Personal Information	Personal Information, as defined in accordance with the <i>Personal Information Protection and Electronic Documents Act</i> (PIPEDA), is data about an identifiable individual. It is information that on its own or combined with other pieces of data, can identify an individual.² Personal Information includes any factual or subjective information, recorded or not, about an identifiable individual. This includes information in any form, such as: • age, name, ID numbers, income, ethnic origin, or blood type • opinions, evaluations, comments, social status, or disciplinary actions • employee files, credit records, loan records, medical records, existence of a dispute between a consumer and a merchant, or intentions (for example, to acquire goods or services, or change jobs)³ Other regulatory frameworks may exist that define Personal Information differently, and client agreements, outside counsel guidelines, and court notices or directives may come with their own definitions of Personal Information and/or information expected to be protected or used for limited purposes by the Firm.

² Office of the Privacy Commissioner of Canada. (n.d.). *Privacy laws in Canada*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/02_05_d_15/#heading-0-0-2-2

³ Office of the Privacy Commissioner of Canada. (n.d.). PIPEDA Requirements in Brief. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda_brief/#personal

Guiding Principles for the Firm's use of AI Systems⁴

Privacy, data protection, confidentiality, solicitor-client privilege & the duty of care	The Firm and its lawyers and staff are obligated by professional codes of conduct, common law, legislation, and client agreements to maintain the confidentiality of client information and take reasonable steps to protect client information from unauthorized access. Lawyers also have an obligation to protect solicitor-client privilege, as is necessary for the preservation of a lawyer-client relationship based on trust. The use of AI Systems by the Firm does not change these fundamental professional obligations.
Human oversight & monitoring	The Firm's AI Systems will be designed in such a way as to enable people managing the operations of the AI System to exercise oversight.
Transparency	The Firm will comply with all legal obligations, including privacy laws, court directives, and client agreements, with regards to identifying and disclosing the purposes for which Personal Information is collected and used by the Firm, including use in AI Systems. As required by regulation, court directive, or client agreement, the principle of transparency may require the Firm to disclose details of the capabilities, limitations, and potential impacts of the Firm's AI Systems. ¹ This includes a level of interpretability and explainability—that is, clarity in the decision-making processes that power the AI System's models—appropriate to the context. ⁵
Fairness & equity	The Firm's AI Systems will be utilized while maintaining an awareness of the potential for discriminatory outcomes. Appropriate actions will be taken to mitigate discriminatory outcomes for individuals and groups. ¹
Safety	The Firm's AI Systems will be assessed to identify harms that could result from use, including through reasonably foreseeable misuse, and security measures will be taken to mitigate the risk of harm relative to the sensitivity of information used by or generated by the AI System. ¹
Accountability	The Firm is responsible for Personal Information under its control and the way that Personal Information is used by the Firm's AI Systems. The Firm is also responsible for the output of the AI Systems and its impact on Stakeholders. The Firm will appoint someone to be accountable for its compliance with all legal obligations, including client agreements. ¹
Validity & robustness	The Firm will monitor and review its AI Systems to ensure that they perform consistently within intended objectives (validity) and are stable and resilient in a variety of circumstances (robustness). ¹
Environmental & societal well-being	The Firm will monitor and review its AI Systems to ensure that their use does not have unintended negative consequences that work against the Firm's values or mission, especially with regards to the health and wellness of Firm employees, clients, the communities in which the Firm operates, and the environment at large. ¹

⁴ The Checklist's Guiding Principles are based in part on PIPEDA's 10 fair information principles. Office of the Privacy Commissioner of Canada. (n.d.). *PIPEDA fair information principles*. https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/p_principle/

⁵ Innovation, Science and Economic Development Canada. (n.d.). *Artificial Intelligence and Data Act (AIDA) companion document*. Innovation, Science and Economic Development Canada. <https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document>

Instructions

The Checklist is a flexible framework designed to guide the Firm in evaluating any AI System that that is, or is expected to be, used within the Firm’s operations.

When asking whether an AI System should be evaluated through the Checklist and to what degree the Checklist’s questions are relevant to the AI System under review, consider:

- Could the AI System process personal or confidential information?
- Could the AI System make decisions or recommendations (including those incidental to the AI System’s primary output or as part of a subprocess)?
- Could any Stakeholders reasonably, contractually, or statutorily expect to know that the AI System is being used, or how the AI System is being used?
- Could the AI System be used in contexts where there is a risk of harm if the AI System does not perform as expected / correctly / consistently?



The Checklist should be initiated as early as feasible in the AI System Lifecycle. For AI Systems not yet deployed, aim to complete it during the evaluation phase, before any piloting or full deployment. For those already in operation, complete the Checklist promptly to identify and address any existing ethical considerations.

Completion of the Checklist should be led by the individual(s), internal organization, and/or department within the Firm that is primarily responsible for the AI System. Collaboration with AI Actors involved in the AI System's deployment is also encouraged to ensure a comprehensive evaluation.

The Checklist is structured around a series of questions, each accompanied by space for comments. Each question allows for flexibility in how responses are recorded, enabling customization based on the specific AI System under review.

A “Yes” typically indicates compliance and/or appropriately managed risk, whereas a “No” suggests further analysis or action may be required by the relevant lawyers, staff members, committee leaders, etc., at the Firm. A “Not Applicable / Not Required” (abbreviated “NA/NR” in the Checklist) response typically indicates that the AI System under review does not raise the ethical considerations of the question, whether because of the nature of the AI System’s inputs and outputs, or because of the nature of the AI System’s generative vs. summative functions, or other reasons determined during the review of the AI System in question.

Checklist

1	Privacy, data protection, confidentiality, solicitor-client privilege & the duty of care	Yes	No	NA/ NR	Comments
1.1	Has the AI System designer provided documentation explaining what data is used to train the AI System, including, but not limited to, the data used historically, data gathered during the operation of the AI System, and data generated from the AI System?	☐	☐	☐	
1.2	Has the AI System designer confirmed whether client data, including outputs derivative of the processing of client data, will be used to train or otherwise improve the AI System?	☐	☐	☐	
1.3	Has it been confirmed what (if any) Personal Information is used in the AI System? (see 4.3)	☐	☐	☐	
1.4	Has a privacy impact assessment (PIA) been completed for the AI System?	☐	☐	☐	
1.5	Has the Firm considered whether the use of this AI System affects any duties (e.g., of integrity, quality of service, courtesy, candour, solicitor-client privilege, etc.) owed to clients, contractual counterparties, opposing parties in litigation, and/or employees?	☐	☐	☐	

2	Human oversight & monitoring	Yes	No	NA/ NR	Comments
2.1	Has the necessary training been conducted for all AI Actors that are or could reasonably be expected to interact with the AI System?	☐	☐	☐	
2.2	Does the Firm have a monitoring and incident response plan in place to detect, report, and address abnormal operations or cybersecurity events related to the AI System? (see 6.2)	☐	☐	☐	
2.3	Does the AI System's designer have a monitoring and incident response plan in place to detect, report, and address abnormal operations or cybersecurity events? (see 6.3)	☐	☐	☐	
2.4	Will this Checklist be stored in a visible and relevant location in relation to the AI System?	☐	☐	☐	

3	Transparency	Yes	No	NA/ NR	Comments
3.1	Has the AI System's designer provided an acceptable level of interpretability and explainability that makes the decision-making processes of the AI System transparent and understandable to the Firm and to any Stakeholders who might reasonably require an explanation?	☐	☐	☐	
3.2	Has the Firm considered whether disclosure to Stakeholders of the use of this AI System and/or informed consent from Stakeholders (possibly including clients or any other data source used as inputs by the AI System) is required?	☐	☐	☐	
3.3	If informed consent has been deemed necessary, has the exact process for obtaining informed consent from Stakeholders been documented, to the extent required under applicable privacy laws?	☐	☐	☐	

4	Fairness & equity	Yes	No	NA/ NR	Comments
4.1	Has the Firm developed a list of Stakeholders who are at-risk of being systematically disadvantaged by the AI System, along with the specific risks for each group?	☐	☐	☐	
4.2	Has the AI System's designer articulated an acceptable quantitative measure or measure(s) of fairness ⁶ ?	☐	☐	☐	
4.3	Has fairness been measured for each piece of Personal Information used in the AI System (see 1.3)?	☐	☐	☐	
4.4	Does the AI System comply with the Firm's equity, diversity, and inclusion principles?	☐	☐	☐	

⁶ For a public library of AI fairness models designed to examine, report, and mitigate discrimination and bias in machine learning, see <https://aif360.res.ibm.com/>, provided by IBM.

5	Safety	Yes	No	NA/ NR	Comments
5.1	Has the AI System passed the Firm's internal IT security assessment?	☐	☐	☐	
5.2	Are protections in place to prevent internal and external manipulation or misuse of the AI System, such as hacks, data breaches, improper use of outputs, etc.?	☐	☐	☐	
5.3	Does the Firm have a documented fallback plan should the AI System result in unexpected behaviour or otherwise fail to produce the process/output intended?	☐	☐	☐	
5.4	Is the AI System compliant with any safety standards or regulations specific to the AI System's operations?	☐	☐	☐	
5.5	Does the contract with the AI System designer explicitly state the ownership of the AI System's intellectual property, including inputs, outputs, derivative works, and training models?	☐	☐	☐	

6	Accountability	Yes	No	NA/ NR	Comments
6.1	Has the Firm identified the primary individual, internal organization, and/or department responsible for the AI System?	☐	☐	☐	
6.2	Has the person(s) responsible at the Firm for monitoring the AI System post-deployment been identified? (see 2.2)	☐	☐	☐	
6.3	Has the main external contact for the AI System's designer been identified? (see 2.3)	☐	☐	☐	
6.4	Have all responsible parties for the AI System been documented in this Checklist and in any additional locations deemed appropriate by the Firm?	☐	☐	☐	
6.5	Is there a documented list of all Stakeholders potentially affected by the AI System?	☐	☐	☐	
6.6	Is there a procedure for notifying Stakeholders (which could include courts, opposing litigants, contractual counterparties, clients, employees, etc.) in the event an ethics issue is uncovered related to the AI System?	☐	☐	☐	
6.7	Do Stakeholders have a feedback channel to enquire about, submit appeals, and request reviews of the AI System?	☐	☐	☐	

6.8	Has the AI System been added to the appropriate Firm inventory or repository of approved tools?	☐	☐	☐	
-----	---	--------------------------	--------------------------	--------------------------	--

7	Validity & robustness	Yes	No	NA/ NR	Comments
7.1	Has the Firm identified what type of AI is being used in the AI System (e.g., generative AI, reinforcement learning, machine learning, etc.)?	☐	☐	☐	
7.2	Are the performance estimates of the underlying model in the AI System, and the uncertainties (if applicable) in those estimates, acceptable given the task context?	☐	☐	☐	

8	Environmental & societal well-being	Yes	No	NA/ NR	Comments
8.1	Has the Firm considered the potential human rights impacts of the use of the AI System?	☐	☐	☐	
8.2	Is the impact of the AI System on job roles, especially those of junior employees, aligned with the Firm's talent strategy?	☐	☐	☐	
8.3	Has the Firm considered retraining and/or upskilling opportunities for employees whose roles may be affected by the adoption of the AI System?	☐	☐	☐	
8.4	Is the environmental impact of the AI System aligned with the Firm's objectives for sustainability?	☐	☐	☐	

This Checklist was developed in November of 2024, and should be reviewed periodically to ensure it remains aligned with developing regulation, including but not limited to the Artificial Intelligence and Data Act, as well as client governing documents and other Firm commitments or obligations.

© Dr. Stephanie Kelley 2024 and © Stewart McKelvey 2024
4156-1990-2291