RGI Regulatory Governance Initiative

Informing Possible Futures for the use of Third-Party Audits in AI Regulations

Benjamin Faveri (benjamin.faveri@carleton.ca)

Graeme Auld (graeme.auld@carleton.ca)

December 10, 2023

This background paper framed discussions at a workshop on AI regulation that took place at Carleton University on November 9, 2023. Themes discussed at the workshop were added to this final version.

Funding for this work comes from a Connection Grant from the Social Sciences and Humanities Research Council of Canada (# 611-2022-0314). The authors also thank Carleton University, the Regulatory Governance Initiative, and the Responsible Artificial Intelligence Institute for their support.

Carleton UNIVERSITY

Recommended citation:

Faveri, B. & Auld, G. (2023). Informing Possible Futures for the use of Third-Party Audits in AI Regulations. Carleton University, School of Public Policy and Administration. http://doi.org/10.22215/sppa-rgi-nov2023

Executive Summary

Canada's proposed *Artificial Intelligence and Data Act* (AIDA) seeks to establish audit requirements for high-impact AI systems under certain circumstances and includes a proposed role for audits in assuring the actions, policies, and measures taken to manage the risks of AI impacts by entities engaged in regulated activities. At their most basic, audits are about checking that rules or expectations are being met by the target of the audit, with some level of confidence. The use of audits has expanded considerably in recent decades, and they have become a feature of many proposed and enacted regulatory approaches for governing the risks of negative AI impacts.

This paper introduces key considerations that ought to be accounted for in devising a regulatory approach for AI that uses audits, whether third-party or internal. It does this based on a review of existing literature that has identified four key areas of consideration:

A. Time and money barriers to entry;

B. Oversight mechanisms to ensure trained and continued auditor competency;

C. Market efficiency versus the potential race-to-the-bottom nature of audit markets;

D. Public regulators creating favourable conditions to raise auditing standards.

We review four cases – the EU's approach to biofuels and data privacy and Canada's approaches to food safety and data privacy – to illustrate different implications of these four considerations. Each case highlights the potential for barriers occurring due to audit requirements and provides examples of ways in which these barriers might be lessened and managed. For AI, the cases show that it will be important not to take for granted the existence of competent audit organizations and auditors, and that ongoing efforts will be needed to ensure a continued supply of professionals capable of performing audits against AI governance standards and regulations. The cases also illustrate that an awareness of the trade-offs and tensions between efficiency and some level of audit

consistency and quality is necessary, and that public regulation can play a role in establishing conditions for raising audit standards over time.

Emerging themes included: (a) a need for attention to the information asymmetries that exist within the AI sector, and how, initially, audits may be as necessary for generating transparency as they are for fostering regulatory compliance; (b) the importance of attention to training and credentialling for individuals that will conduct AI audits; and (c) the need for regulation to oversee both the competencies and professionalism of audit organizations as well as the functioning of audit markets overall.

RGI
Regulatory Governance Initiative

Table of Contents

Introduction

Artificial intelligence (AI) systems are developing rapidly. The benefits of these developments stand to have far-reaching effects. AI can significantly improve social, economic, and environmental welfare by generating novel and efficient solutions for problems of access to healthcare, medical diagnostics, and environmental management. But AI systems also create new risks of harm that have raised concerns and motivated various efforts to develop public and private regulatory standards. AI systems can displace labour, exacerbate discrimination, create black box decision-making, remove human judgement and accountability from decision-making, impact the safety or human environments, and exacerbate environmental degradation (Auld et al., 2022).

To increase AI systems' benefits and reduce their risks of harm, hundreds of AI governance initiatives have emerged (Jobin et al., 2019; OECD, 2022). These initiatives have taken the form of national strategies, legislation and regulation, certification programs, international and national standardization developments, and government directives. Much remains underspecified in these emerging governance initiatives. But a consistent theme is the potential role of third-party audits and auditors in assessing the risks of harm and regulatory compliance of AI systems. Canada's *Directive on Automated Decision Making* (DADM), *Algorithmic Impact Assessment* (AIA), and recently proposed *Artificial Intelligence and Data Act* (AIDA) all include language around audits, peer-reviews, or self-assessments, all of which we conceptualize as some form of internal or external verification against a set of criteria (an audit). However, little is specified about the roles, processes, competency requirements, costs, timeframes, guiding policies, public sector intervention, etc. that will govern the role of audits for AI systems and their risks of harmful impacts. As Canada pushes forward with these AI audit and audit process efforts, it is crucial to clarify these areas and present a path forward.

The aim of this background document is to begin an examination of how other industries and regions' audit and audit processes provide a basis for discussing how Canada might use this regulatory mechanism for assessing and regulating the risks of AI harms. The assessment of these other industries and regions' audit and audit processes focuses on four issues:

1. First, the constraints and barriers created by the time and money barriers involved in conducting audits. We know from experience that audit requirements can create barriers to small and medium sized businesses due to audit fixed costs and the information demands required for assessing and demonstrating compliance. How might these concerns be managed?

2. Second, successful audits require that audit organizations and individual auditors have the necessary technical and operational expertise and capacities to check whether standards are being met or risk thresholds are or are not being surpassed, and that they are preforming these functions and judgements free of conflicts of interest. What can be done to ensure there is sufficient oversight of audits and audit processes to maintain quality control over these processes?

3. Third, the use of third-party audits may offer flexibility and choice to businesses that are demonstrating legal compliance, creating the potential for market efficiencies. Yet, competition among third-party auditors may create a race-to-the-bottom dynamic that harms the quality of audits performed overall. To what extent do we observe a trade-off between market-efficiency and audit quality in other use cases?

4. Finally, the role of auditors and the function of audit markets can be the focus for government oversight. What options are available to public regulators to prevent a race-to-the-bottom dynamic and potentially raise audit standards and the quality of audit practices?

To shed light on these questions, we proceed as follows. We begin with a three-part background that introduces: (A) third-party audits and audit processes; (B) the unclarified nature of third-party audit and audit processes in Canada's AI governance efforts; and (C) current AI audit and audit process efforts. A second section motivates our four guiding questions by discussing some important academic findings about the role and consequences of audits, especially third-party audits. The third section reviews our four initial case studies. The cases are: (A) the European Union (EU)'s approach to regulating sustainable biofuels; (B) the EU's approach to regulating data privacy; (C) Canada's approach to regulating food safety; and (D) Canada's approach to regulating data privacy. The assessments of each case are not comprehensive and exhaustive reviews of these

areas of regulatory governance. Rather, they place focused attention on the role of audits with the intention of highlighting differences that have consequences for the four key areas of consideration identified above. The paper concludes with reflections on lessons from the cross-case comparisons, emerging themes, and outstanding questions.

This paper should not be read as an endorsement of audits and their potential role in the regulatory oversight of harmful AI risks. Rather, it is meant to inform decision-makers about the varied ways in which audits have been and can be used, as well as the consequences of these choices. Other forms of oversight and assurance are possible and merit consideration as the Canadian government finalizes its regulatory approach to high-impact AI systems.

Background

A. Third-Party Audits and Audit Processes

Back in the late 1990s, Michael Power's (1997) book *The Audit Society* noted the rising attention to and practice of audits in the United Kingdom; this practice has only since expanded across jurisdictions and issue areas, spanning from the world of technical standards and conformity assessment bodies to internal and third-party audits of businesses' social and environmental practices (Büthe & Mattli, 2011; Loconto & Busch, 2010). At their most basic, audits are about checking that rules or expectations are being met by the target of the audit, with some level of confidence. To accomplish this, audits are organized to include certain basic attributes: "independence from the matter being audited; technical work in the form of evidence gathering and the examination of documentation; the expression of a view based on this evidence; a clearly defined object of the audit process" (Power 1997, p. 5).

What gets audited – the defined object of the audit – is an important starting point. Audits are not open-ended investigations or evidence gathering exercises; rather, they are about assessing practices against a specific standard. In the context of food safety, standards like the Hazard Analysis and Critical Control Points (HACCP) system, audits focus on procedures and plans that identify risks and control measures to be taken in situations where monitoring identifies control limits are exceeded (Skogstad, 2008, p. 189). In another example, the Rana Plaza factory

collapse in 2013 that killed 1134 workers raised serious questions about the effectiveness of the Business Social Compliance Initiatives (BSCI) Code of Conduct which had been the basis for an audit of the Rana Plaza facility conducted by TÜV India. Ultimately, questions of legal liability were avoided because the Code of Conduct did not consider the structural integrity of the building as within the scope of the audit (Verbruggen, 2022).

The idea of a third-party audit – that is, being external to the relations and activities being audited – is central to the way independence and competence are understood and practiced. It involves questions of both ethical conduct and professionalism for individual auditors, as well as questions about the interests of the organizations that manage the audit process, what we term the audit organizations. With individuals, professional credentialling processes – like becoming a chartered professional accountant – offer one way to oversee and assure that independence and competence are maintained. With organizations, accreditation rules and processes are often designed to ensure audit organizations are managed to keep potential conflicts of interest in check (Auld & Renckens, 2023).

Qualities of individuals and organizations are equally relevant for audit processes – that is the processes used to gather evidence, evaluate that evidence, and make an ultimate determination based on the evidence. These processes can vary widely from document checks, field visits, remote or virtual visits, to stakeholder meetings all with the intention of seeking evidence of practices that are (or are not) consistent with expectations. Individuals require expertise and competencies that match the technical questions raised by the subject under audit. Organizations must have the capacity to organize and deliver an audit. Credentialing and accreditation are again a means by which expertise, competencies, and organizational capacity can be assessed and overseen.

B. Unclarified Third-Party Audit and Audit Processes in Canada's AI Governance Efforts

Canada's AI governance initiatives began in 2017 with the *National AI Strategy's* phase one launch and early draft writing of what would later become the *Directive on Automated Decision-Making* in 2019. This Directive applied to federal institutions and sought to ensure that only AI systems in production and that make administrative decisions or a similar client-related assessment "are deployed in a

manner that reduces risks to clients, federal institutions and Canadian society, and leads to more efficient, accurate, consistent and interpretable decisions made pursuant to Canadian law."[1] In 2022, the *National AI Strategy's* second phase was launched,[2] and the draft *Artificial Intelligence and Data Act (AIDA)*[3] was proposed.

The *AIDA's* draft has two stated purposes. The first is to provide "common requirements, applicable across Canada, for the design, development and use of [AI] systems" to regulate Canada's interprovincial and international trade and commerce of AI systems. The second is "to prohibit certain conduct in relation to artificial intelligence systems that may result in serious harm to individuals or harm to their interests."[4] Harm is currently understood in the draft as physical or psychological and damages to property and economic loss.

Much remains unspecified in this *AIDA* draft, despite Minister Champagne's recent letter detailing several AIDA amendments (Champagne, 2023). But certain contours of a future regulatory regime are apparent. One reasonably clear component is the method proposed for assessing and verifying AI systems' risks and mitigation strategies for those risks. That is, there will be some role for third-party auditors as the *AIDA* draft mentions auditors in a few sections. Section 7 requires those responsible for an AI system to assess whether it is a high-impact system. The meaning of high-impact remains unspecified in this draft. Under the previous draft, a "*high-impact system* means an artificial intelligence system that meets the criteria for a high-impact system that are established in regulations."[5] Now, Minister Champagne's recent letter includes a Schedule (to be added to AIDA as "Schedule 2") for determining whether an AI system is high-impact or not. This schedule seems to base its evaluation of an AI system on the context in which it is used. For instance, "the use of an [AI] system in matters relating to determinations in respect of employment, including recruitment, referral, hiring, remuneration, promotion, training, apprenticeship, transfer or termination" would be categorized as a high-impact AI system.

---

[1] https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592
[2] https://www.canada.ca/en/innovation-science-economic-development/news/2022/06/government-of-canada-launches-second-phase-of-the-pan-canadian-artificial-intelligence-strategy.html
[3] https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading
[4] https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading
[5] https://www.parl.ca/DocumentViewer/en/44-1/bill/C-27/first-reading

When an AI system meets the definition of high-impact as specified in these amendments, then the entity responsible for that AI system must "establish measures to identify, assess and mitigate the risks of harm or biased output" (section 8) and "monitor compliance with these established measures and their effectiveness" (section 9). Under section 15, if the AI and Data Commissioner has reasonable grounds to believe either of these or any other section between 6-14 were contravened, they may require those responsible for the AI system to:"(a) conduct an audit with respect to the possible contravention; (b) require, by order, that the person conduct the audit; or (c) require, by order, that the person engage the services of an independent auditor to conduct the audit." In all instances, the audit must be conducted by someone who meets the qualifications prescribed by regulation under section 36(f). Yet, these auditor qualifications are unknown and left up to forthcoming regulations.

In March 2023, an *AIDA* "companion document"[6] was released to guide industry and regulators on the intent of the *Act* and how it *should* work while they wait for the forthcoming regulations. On April 24, 2023, *AIDA* passed the House of Commons' Second Reading.[7] As this Bill continues through the legislative process without regulations to clarify third-party audits and audit processes, it becomes ever more important to think through possible audit and audit process challenges and how other industries and regions' have addressed and resolved their audit and audit process challenges.

C. Current AI Audit and Audit Process Efforts

While much national regulation and legislation has ignored the clarification of AI audits and audit processes, the AI industry has not. Firms like The Responsible AI Institute,[8] ForHumanity,[9] BABL,[10] the International Association of Privacy Professionals (IAPP), Ulysses,[11] and Eticas[12] have all started to create and

[6] https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document
[7] https://www.parl.ca/legisinfo/en/bill/44-1/c-27
[8] https://www.responsible.ai/
[9] https://forhumanity.center/
[10] https://babl.ai/courses/
[11] https://www.ulysses-ai.com/services
[12] https://eticas.tech/algorithmic-audits

implement varying AI audit and audit processes. The Responsible AI Institute is nearing the end of a pilot with ATB Financial and the Standards Council of Canada (SCC) to audit ATB Financial against the Responsible AI Institute's *Responsible AI Certification Program's* requirements.[13] ForHumanity and BABL have developed, released, and certified individuals against various professional AI audit certifications, although these professional certifications are not accredited nor created against existing international AI standards, like ISO/IEC CD 42006. Conversely, the IAPP, which is a highly regarded industry association in the privacy space and offers sought-after privacy professional certifications (like the *Certified Information Privacy Professional* (CIPP)), will be releasing an *AI Governance Professional (AIGP) Certification* in the first few months of 2024. The AIGP will include material on AI audits, international standards, and risk management, among other criteria (see AIGP Book of Knowledge). And Ulysses and Eticas are boutique private consulting firm that offers AI system audits throughout the entire AI system lifecycle, although they do not offer a certification mark for passing their audits.

Despite these firms generating considerable market demand for their varying audit and audit related services, they do not seem to have considered or positioned themselves to address and navigate the varying challenges presented by established industries and regions' audit and audit processes. For instance, ForHumanity, BABL, and IAPP will all soon be offering professional certifications for AI audits, competing for which professional certification becomes "adopted" by industry and looked for when accredited auditors audit AI systems. While ForHumanity and BABL have a head start on professional AI audit certification offerings, IAPP has far more industry weight, has publicly released their upcoming AIGP certification required Body of Knowledge, and actively updates their existing certifications to current regulatory, legislative, and international standardization requirements, even offering country/region-specific privacy professional certifications (i.e., Canada, the US, and EU). Similarly, RAII, Ulysses, and Eticas will each be offering auditing services (at least for the time being, RAII may opt to license their certification mark to accredited auditors and distance themselves from auditing against their own certification). While RAII is clearly ahead given how long they have been in the industry, their industry ties through

[13] https://www.scc.ca/en/news-events/news/2022/scc-launches-accreditation-pilot-for-ai-management-systems

their various member organizations, and their inclusion of current regulatory, legislative, and international standardization requirements in their AI system audit requirements, Ulysses or Eticas could become a larger player if they continue to specialize in AI audits and RAII distances themselves as auditors. In a new effort to avoid this possible competition issue, on December 7th, 2023, BABL, Eticas, ForHumanity, and some other AI-focused organizations have joined up to create the International Association of Algorithmic Auditors[14] that will offer a professional certification for AI auditors. While these efforts help meet the potential increasing industry demand for competent auditors, exploring how other industries and regions' third-party audit and audit processes have addressed established audit and audit process challenges may help existing AI audit firms navigate and position themselves to address these eventual challenges.

Motivating our Guiding Questions

Auditors, both internal and external, are frequently used in public regulation to perform assessment functions. The design of these regulatory systems can have important consequences that are separate from how stringent the rules are for what constitutes a high-impact AI system. We know several things about audits and audit processes from existing research, and we use this existing knowledge as the basis for questions we explore in the case study section that follows.

A. Time and Money Barriers to Entry

The use of audits can be resource demanding. They take time (Renckens & Auld, 2022) and money (Michaelowa & Jotzo, 2005; Ponte, 2008), and they are understood to generally favour larger operators that can more easily cover the fixed costs that audits entail (Auld et al., 2008). Consistent with economic theories of public regulation (Peltzman, 1976; Stigler, 1971), we can think of audit requirements creating barriers to entry that favour incumbent firms and that in turn may reduce innovation that could arise were small-and-medium enterprises able to enter the market. Thus, from a regulatory perspective, understanding the extent to which this can be overcome and managed requires attention. What do the cases tell us about the ability to reduce these forms of barriers to entry, especially those created by audit requirements?

[14] https://iaaa-algorithmicauditors.org/

B. Oversight Mechanisms to Ensure Trained and Continued Auditor Competency

Auditors, especially third-party auditors, require oversight to ensure they are acting independently and that they are sufficiently competent to perform their assessments. Experience from accounting and sustainability auditing fields highlights the importance of these competencies (Bishop & Carlson, 2022; Short et al., 2016; Toffel et al., 2015), and that these do not exist without effective efforts to train and professionalize individual auditors. Given these considerations, what can be done to ensure there is sufficient oversight of audits and audit processes to maintain quality control over these processes? What forms of policy intervention are needed to generate sufficient supply of capable audit organizations and audit professionals for an issue like the risks of harmful AI?

C. Balancing Market Efficiency and Third-Party Auditing's Race-to-the-Bottom Nature

The supply of both audit organizations and individual auditors cannot be taken for granted. One advantage of third-party rather than internal auditing is the expected benefits of private-sector efficiency. Businesses that seek audit services can benefit from price competition among audit organizations in the market. However, efficiency benefits rely on specific market conditions, such as competition, which itself can create unintended consequences like diminishing rigour of their assessments (e.g., see discussion of this problem with tailing dam assessments done by private technical inspectors in the mining sector, (Saes & Muradian, 2021)) and races to the bottom on standards more generally.

Thus, we must consider what we can term the audit market and the supply of individual auditors and audit organizations in this market. The effective and efficient operation of third-party audits partly rest on the functioning of these audit markets – that is, in theory, the sufficient supply of competent auditors, both individuals and organizations. Rules, for instance, that limit the number of repeat audits that can be performed for the same audit target, hinge on a sufficient supply of auditors; similarly, the ability for price competition to lead to efficient delivery of audit services requires that there are sufficient audit organizations in the market that can viably compete.

Balancing these benefits and costs is an essential consideration. But, how to intervene is not always clear, given establishing requirements for auditor entry can themselves create barriers that empower certain businesses and exclude others. For instance, Sinclair (2014, pp. 42-45) details how the US Security and Exchange Commission rules in the 1970s supported incumbent rating agencies and limited the opportunities for newer competitors. Thus, market entry rules may (un)intentionally affect audit market structure. Given these concerns and trade-offs, what are essential considerations for overseeing third-party audits for AI risks?

D. Public Regulators Creating Favourable Conditions to Raise Auditing Standards

Conversely to the last point, evidence from cases does suggest that private standards and audit processes can be overseen in ways by public regulations to create conditions that favor raising audit standards over time. In the European Union (EU), for instance, the public organic standard serves as a floor; third-party auditors for organic agriculture must meet these standards but can require additional practices (Renckens, 2020). Certain scholars have thought of this problem through the idea of iterative experiments, where a central regulator seeks to work with third-party auditors to foster decentralized experimentation, ex-post stocktaking, and peer-review to identify promising ways to address the problem at hand (Sabel & Zeitlin, 2008). Could such a model inform how audits might play a role in building an information base for more effective standards and AI oversight in the future? What do previous experiences tell us about the potential for creating conditions favourable for raising standards?

Cases Studies

Our four case studies are presented below to explore: (A) time and money barriers to entry; (B) oversight mechanisms to ensure trained and continued auditor competence; (C) balancing market efficiency and third-party auditing's race-to-the-bottom nature; and (D) public regulators creating favourable conditions to raise auditing standards.

1. The EU's Sustainable Biofuel Audit Approach

In the early 2000s, the EU began to promote biofuels adoption in its market for transportation fuels as one means to reduce greenhouse gas (GHG) emissions. Directive 2003/20/EC detailed the first efforts to promote renewable fuels, with the aim of "promoting the use of biofuels or other renewable fuels to replace diesel or petrol for transport purposes in each Member State" (Article 1). Member States were charged with ensuring renewable fuels gained market share, with an indicative target of 2% for all petrol and diesel (based on energy content) by the end of 2005, rising to 5.75% by the end of 2010 (Article 3). Member States had leeway to adopt specific targets other than the indicative ones, but this needed to be justified to the European Commission (EC) based on constraints like limited production capacity or the existence of other national policies promoting renewable energy consistent with the Directive's aims (Article 4).

In the years that followed, renewable fuels became a more central consideration in relation to climate change, with more questions being raised about the downsides of renewable fuels in the form of limited additionality, land use changes, and social impacts. Renewable fuels were also more directly tied to the EU's 2020 targets of reducing GHG emissions by 20% compared to a 1990 baseline (Renckens, 2020, pp. 104-105).

Directive 2009/28/EC set out a common framework for the promotion of renewable energy in the transport sector, including mandatory national targets (Article 1). By 2020, renewable energy used in transport was to constitute 10% of energy sources for transport in Member States (Article 4). The Directive also introduced specific requirements for sustainable biofuels and bioliquids (Article 17), most importantly, the expectation that these renewable fuels would meet increasingly stringent requirements for their GHG emissions savings. These were initially set at 35%, meaning the fuels had to generate 35% less emissions than non-renewable fuels, if they were to count towards national targets or be eligible for any financial support. This would be raised to 50% as of January 1, 2017, and 60% as of January 1, 2018 (Article 17(2)). Other restrictions included rules against obtaining feedstock for renewable fuels from "land with high biodiversity value" such as primary forests, areas designated for nature protection, grasslands with high levels of biodiversity, areas with high carbon stock, and peatlands (Article 17(3)-(5)).

To demonstrate compliance with these sustainability criteria, the Directive required Member States to ensure operators in their jurisdiction fulfill the Directive's legal obligations. For the Member States, this meant developing measures to elicit reliable information from operators, and that operators "arrange for an adequate standard of independent auditing of the information submitted, and to provide evidence that this has been done" (Article 18(3)). The EC (as set out in Article 18(4)), played a role in determining acceptable private voluntary third-party auditing schemes that operators could use as the basis for supporting the adequacy of their data and their compliance with the Directive's sustainability requirements (in Article 17 (2)-(5)). Seeking and obtaining third-party certification from such an approved scheme would substitute for any information requirements a Member State might establish (Article 17(7)).

In 2010, the EC released the Communication on Voluntary Schemes and Default Values in the EU Biofuels and Bioliquids Sustainability Scheme that detailed the approach and requirements it would use when vetting voluntary schemes. Eligible programs could be private schemes or ones developed by governments; they would be assessed against the sustainability criteria set out in Directive 2009/28/EC, as explained above; and they could be recognized, even if another scheme already covered a given feedstock and sustainability issue. In addition, schemes would be evaluated on how they handled document management (sec. 2.2.1), and how their audits were performed to ensure independence. Other requirements covered ensuring that the auditors were external to the operator, that the third-party audit organizations had sufficient general skills to do the audits and individual auditors were competent in the relevant areas of sustainability (sec. 2.2.2), and that the scheme had in place chain of custody systems to deal with mass-balance evaluations (sec. 2.2.3).

Additional procedural oversight of voluntary schemes was added in 2015 with the adoption of Directive (EU) 2015/1513. Most importantly, schemes would now need to publish a list of their accredited audit organizations and note the accreditation body responsible for overseeing each auditor (Article 18). Further reporting requirements to the EC were added, and Member States were required to

recognize voluntary schemes as equivalent to Member States' schemes in relation to the assessment of the sustainability criteria in the Directive.[15]

The number of approved schemes has shifted over the last decade. Seven schemes were initially approved in 2011, many of which were private schemes that predated the renewable energy directive. As of 2014, Renckens (2020) reported that 19 schemes had received approval, with a higher proportion of industry association and business led schemes (Table 4.3, pp. 120-21). Currently, the number of schemes has dropped to 15, with an additional 9 currently seeking approval.[16]

A. Time and Money Barriers to Entry

The EU had concerns about Directive 2009/28/EC's verification procedure implications for smaller operators, noting (in Article 18(3)) that when developing guidance on what should be reported to demonstrate compliance, it was necessary to ensure that "the provision of that information does not represent an excessive administrative burden for operators in general or for smallholder farmers, producer organizations or cooperatives in particular."

In the 2010 Communication about voluntary schemes, the EC included certain provisions related to barriers to entry that third-party audits might create. First, the approval process notes that group auditing can be acceptable "for smallholders, farmers, producer organizations and cooperatives" and can involve sampling according to appropriate standards. Assessing land use or GHG savings can only be done under such circumstances when there is reasonable homogeneity in the areas and production systems under audit (sec 2.2.2).[17] Second, the EC established default values for GHG savings that operators could use in lieu of new calculations. These default values were set at conservative levels to ensure emissions savings occurred, while also serving to reduce the need for original and potentially costly operator-specific calculations (sec 3). These are indicative of measures taken to lower the potential auditing costs faced by smaller operators.

[15] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32015L1513&qid=1695670024994#d1e1112-1-1
[16] https://energy.ec.europa.eu/topics/renewable-energy/bioenergy/voluntary-schemes_en
[17] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A52010XC0619%2801%29

B. Oversight Mechanisms to Ensure Trained and Continued Auditor Competence

As noted above, the Communication on voluntary schemes from 2010 detailed specific considerations the EC was to consider in evaluating schemes. Section 2.2.2 deals with the audit procedures and discusses ways in which to check that schemes comply. This includes discussion of various indicators for the EC's concerns with independence, external audits, auditing competencies held by the organization, and substance expertise held by the individual auditors.

Further oversight of the schemes now exists, as detailed in the Assessment Protocol for voluntary schemes (updated in 2022). As compared to the Communication document from 2010, greater specifics are now detailed in this protocol, including on the issue of auditor competencies that covers the appropriate process for selecting audit teams or individual auditors and criteria for their specific competencies. Additionally, schemes are now expected to have in place "training courses for certification bodies, covering all aspects relevant to the scope of the scheme" and processes for monitoring the "training status" of auditors to ensure they remain up to speed on the expertise needed for the audits. In this way, the EU has developed considerably more extensive oversight of the voluntary schemes' engagement with competent auditors.

C. Balancing Market Efficiency and Third-Party Auditing's Race-to-the-Bottom Nature

Private schemes offered several market efficiency benefits for the EU as they helped the EU fairly deal with imported biofuels, which like EU sources, would need to be third-party audited against an approved scheme (Renckens 2020, p. 113). Equally, the focus on mutual recognition among schemes helped ensure equal treatment across the EU for operators seeking to sell renewable fuels. This attention to market efficiency, however, did lower ambition, where schemes that developed later could pitch their standards directly in relation to EU requirements. As Renckens (2020) explains, this has set up a direct competition between multi-stakeholder schemes and potentially more streamlined and less pluralistic schemes led by industry associations and businesses: "This decision has resulted in a situation in which certification schemes that spend valuable resources on establishing a credible stakeholder-driven initiative are competing with schemes that are more one-sided in terms of interest representation and stakeholder involvement" (p. 122).

D. Public Regulators Creating Favourable Conditions to Raise Auditing Standards

As early as Directive 2009/28/EC, there were provisions concerning the practice of audits by the private schemes recognized by the EU. The EC was meant to only recognize schemes that met "adequate standards of reliability, transparency, and independent auditing" (Article 18 (5)).[18] These standards were raised in 2015, when the EC introduced regular annual reporting, where schemes must provide details on "their audits, procedures for addressing noncompliance, stakeholder involvement, feedstock and biofuels that were certified, and rules for accreditation" (Renckens 2020, p. 124). In this respect, there has been a notable effort within the EU's approach to raise the expectations for audits based on the experience gained from the roll out of the program.

2. The EU's Data Protection Audit Approach

The EU's data protection audit approach has three levels, presented in hierarchical order. First, if an EU Institution (EUI) is determined to be using risky data-related processes, the European Data Protection Supervisor (EDPS) will audit that EUI to determine their Regulation (EU) 2018/1725 compliance. Second, if enough complaints are submitted against a particular firm or government body, that firm's Member State's Independent Supervisory Authority (ISA) will conduct an audit to determine that firm or government body's GDPR compliance. And third, to avoid the first two audits, firms, government bodies, and EUIs use internal or third-party audits to demonstrate their GDPR (for firms and Member State government bodies) or Regulation (EU) 2018/1725 (for EUIs) compliance through data protection impact assessments (DPIA) – the assessment that auditors audit against. Each level is described in more detail below with the case study focusing on the third level of the EU's data protection audit approach, the use of internal and third-party auditors to demonstrate regulatory compliance.

The EU's Regulation (EU) 2018/1725, commonly called the "GDPR for EU Institutions," created the EDPS to oversee, advise, ensure a coherent approach to personal data protection throughout the EU and EUIs, and monitor new technologies that could affect protection of personal data (like AI), among other

[18] https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=celex%3A32009L0028

responsibilities. The EDPS selectively performs audits on EUIs to carry out its responsibilities.[19] These selections are based on the EDPS's risk analysis procedure that includes factors like categories of data processed, number of complaints against them, and general cooperation with the EDPS. Each EUI being audited is outlined in the EDPS's annual audit plan and will be carried out according to their audit guidelines and policy. General information about these audits will be made public in the EDPS's annual reports and through their website. Outside of EDPS audits, EUIs can complete internal or third-party audits to demonstrate their Regulation (EU) 2018/1725 compliance through DPIAs.

At the Member State level, the EU's (2016) GDPR requires that Member States establish an *Independent Supervisory Authority (ISA)* to oversee all establishments within their Member State and any establishments that substantially affect data subjects of their Member State.[20] Some other ISAs' responsibilities include: monitoring and enforcing the application of the GDPR; handling and investigating complaints from data subjects, organizations, and other bodies; encouraging the establishment and approving the criteria of data protection certification mechanisms and seals and marks; and ensuring data protection impact assessments are conducted when required by the controller (the person, body, agency, etc. processing the data; i.e., firms); among several other responsibilities (see GDPR Articles 35, 36, 42, 43 and all of Chapter 6). Under ISAs' investigative powers, they can carry out data protection audits and impose administrative fines or temporary or definitive limitations or bans on data processing controllers when legally justified.

While ISAs and the EDPS can audit firms, government bodies, or EUIs when enough complaints are logged against them or their data practices are found to be above a certain permitted risk threshold, the norm is for these establishments (aside from ISAs and the EDPS) to complete data protection impact assessments (DPIAs) to demonstrate their ongoing GDPR and Regulation (EU) 2018/1725 compliance. These DPIAs are either completed by internal or third-party auditors, and are based on various criteria such as technical standards, checklists, best

[19] For a complete list of EUI and bodies, see: https://european-union.europa.eu/institutions-law-budget/institutions-and-bodies/search-all-eu-institutions-and-bodies_en
[20] For a complete ISA list, see: https://edpb.europa.eu/about-edpb/about-edpb/members_en#member-se

practices, and charters. For example, Bureau Veritas, a third-party auditing firm, offers their *Data Protection Certification*, a voluntary certification program based on their own technical standard of what constitutes GDPR compliance, and, if passed, remains valid for three years. Conversely, the Scottish Government conducted an internal DPIA of their *Scottish Household Survey* practices using a set of internally developed risk management controls to demonstrate GDPR compliance.

A. Time and Money Barriers to Entry

Firms, government bodies, and EUIs (establishments) are encouraged to demonstrate their GDPR and Regulation (EU) 2018/1725 compliance through a certification mark earned by passing a data protection-related audit, often using a DPIA as the audit's assessment. The time and money barrier to entry for GDPR or Regulation (EU) 2018/1725 compliance depends on whether these audits are conducted internally or externally. Internal audits require these establishments to employee auditors with the necessary specialized knowledge to conduct these audits. Given the specialized knowledge and training needed to complete these audits, employing these people is costly while training existing employees to gain this knowledge is likely less costly but requires more time, either option may not be within small or medium sized firms' budgets or ability. Conversely, hiring external auditors to complete DPIAs faces a similar trade-off, they are costly given their specialized knowledge and experience in the field, but are hired to complete one audit (unless retained for annual re-certification/surveillance audits), making hiring them, at least in theory, more time efficient to demonstrate GDPR or Regulation (EU) 2018/1725 compliance compared to internal auditors who require initial training or have additional responsibilities within their role.

B. Oversight Mechanisms to Ensure Trained and Continued Auditor Competence

Like Canada's data privacy and data governance oversight mechanisms for ensuring trained and continued auditor competence (discussed below), the IAPP offers a CIPP-EU certification program that includes auditing of privacy programs (data protection being subsumed within) in its Body of Knowledge. Similarly, the Data Protection Institute offers a *Data Protection Auditor Certification Training* that focuses on training internal and external auditors to audit against ISO/IEC 17065, 17067, 19011, and 27001 and understanding how ISAs conduct GDPR inspections, among several other criteria. Passing this course provides the *GDPR Auditor*

Certificate[21] and is sought after, among other similar certifications, when hiring internal or external auditors. Similarly, the EU GDPR Institute – a think tank focused on training and certification for individuals, professionals, and companies – offers several GDPR-related certifications such as the *GDPR*,[22] *Codes-of-Conduct*,[23] and *GDPR Executive Certifications*.[24] Each of these certifications programs ensure EU data protection auditors, data controllers and processors, and executives are trained on relevant international standards, charters, and best practices to provide a series of controls and oversight measures for private and public organizations to monitor and address data protection issues.

C. Balancing Market Efficiency and Third-Party Auditing's Race-to-the-Bottom Nature

Member States' ISA's and the EU's EDPS provide downward pressure on firms, government bodies, and EUIs to demonstrate their GDPR and Regulation (EU) 2018/1725 compliance continuously and credibly under threat of public investigation or audit results. DPIAs, their audits, and subsequent certification marks if passed, are the typical method used to demonstrate this regulatory compliance. However, DPIA criteria are not provided in either of these regulations, allowing these criteria to vary across different DPIAs. This allowed varied criteria provides the opportunity for loosened data protection auditing standards as some DPIAs can be less stringent, costly, or time and administratively burdensome than others, leaving the potential for a race-to-the-bottom for third-party auditing firms and internal auditing teams using these DPIAs as the basis for their audits.

D. Public Regulators Creating Favourable Conditions to Raise Auditing Standards

Currently, public regulators are not creating favourable conditions to raise auditing standards and are not positioned to do so. This race-to-the-bottom potential and DPIA variances could be minimized if public regulators outlined some baseline criteria necessary for all DPIAs, much like PIPEDA's *10 Fair Principles* in Canada discussed below, thereby raising, or creating consistent EU data protection auditing standards. Alternatively, these variances could be

[21] https://www.dp-institute.eu/en/courses/data-protection-audit-compliance/
[22] https://www.eugdpr.institute/obtaining-a-eugdpr-institutes-gdpr-certification/
[23] https://www.eugdpr.institute/the-eugdpr-institutes-codes-of-conduct-and-certification/
[24] https://www.eugdpr.institute/executive-certification/

partially avoided if the various organizational requirements to sufficiently conduct a data protection or related audit were outlined, such as Article 37 in the recently enacted *Digital Services Act* (2023) and its application to large language models.

3. Canada's Food Inspection Audit Approach

The Canadian food inspection audit approach has been characterized as a strategy of regulation for competition, wherein the main motivations are ensuring food safety oversight ensures access to global markets, and tries to harmonize regulations with significant trading partners (Skogstad, 2008, pp. 180-181). Pursuing this strategy has been complicated by the division of powers within the Canadian federation. "At least two, and sometimes three, orders of government are responsible for enforcing food safety standards, recommendations, and investigating complaints about unsafe food products and seizing and recalling such products" (Skogstad 2008, p. 191).

Putting aside some of these complexities, we focus on two parts of the Canadian food inspection regime for illustrative purposes. The first deals with food safety and is covered by the (2019) *Safe Food for Canadians Act (*SFCA*)*,[25] which introduced new regulations that consolidated and updated what had been 14 separate food-related regulations set by the federal government (Charlebois et al., 2021). The SFCA's key provisions are set out in Article 20 on Registrations and Licences, which detail the powers needed to create regulatory licencing conditions for persons or establishments operating specific food business activities that involve inter-provincial and territorial or international food trade – establishments that fall under federal responsibility.

To hold a licence, an establishment (or individual representing that establishment) must prepare, record, and implement a preventive control plan (PCP; SFCA, Section 89). These PCPs are meant to identify how food hazards and risks are overseen and controlled. Preventive controls for food safety are based on the *General Principles of Food Hygiene* adopted by Codex Alimentarius[26] and the

[25] https://laws-lois.justice.gc.ca/eng/acts/S-1.1/index.html
[26] https://www.fao.org/fao-who-codexalimentarius/sh-proxy/en/?lnk=1&url=https%253A%252F%252Fworkspace.fao.org%252Fsites%252Fcodex%252FStandards%252FCXC%2B1-1969%252FCXC_001e.pdf

Terrestrial Animal Health Code – Slaughter of Animals from the World Organization for Animal Health.[27] Licenced establishments must generate a PCP that identifies and explains the control measures to be taken when risks to food or humane treatment of food animals arise. However, exceptions exist, particularly for smaller businesses with gross sales under $100,000 per annum.

Throughout the documentation on this new regulatory regime, the Canadian Food Inspection Agency (CFIA) notes that there are many existing industry and voluntary guidelines and approaches that can be used to develop and implement a PCP. These include the (2005) ISO 22000 Food Safety Management Systems standard or the Food Safety Systems Certification (FSSC) 22000, which builds from the ISO standard but adds additional requirements. The latter of these standards is recognized by the Global Food Safety Initiatives (GFSI) – an industry wide collaboration that sought to benchmark food safety standards and certification processes to reduce, among other things, the duplication of audits. Establishments are given legal flexibility to determine the approach best suited to them, although, as we note below, compliance is often mandatory, based on private procurement strategies of lead firms in the food value chain (i.e., retail and grocery stores, see Havinga & Verbruggen, 2017).

The new licencing regime has also been designed to help the CFIA collect further establishment specific information on a more comprehensive basis. The SFCA's 2019 changes meant a larger number of establishments came under the oversight of CFIA – approximately 50,000. The licencing process has the benefit of ensuring CFIA knows who it is overseeing and what kinds of operations they are running. They use this information as part of a new risk-based inspection approach that seeks to allocate their limited oversight resources to the higher-risk establishments.[28] Establishment characteristics like the type of commodity are the first input into the risk assessment. A second group of considerations are termed mitigating factors; these include consideration of third-party audits against private industry and voluntary standards like different forms of HACCP systems, ISO 22000, FSSC 22000, or other GFSI recognized systems. Such consideration for

[27] https://www.woah.org/en/what-we-do/standards/codes-and-manuals/terrestrial-code-online-access/

[28] https://inspection.canada.ca/about-cfia/cfia-2025/era-models/era-model-for-food-establishments/understanding-the-era-food-model/eng/1508787947521/1508787947985

private certification was first introduced in a policy adopted in September 2015, which stated that: "In determining the level of risk associated with a regulated party of their establishment, the CFIA may assess the requirements of a private certification scheme used by the regulated party against food safety regulatory requirements and factor the assessment results into its risk-based planning and prioritization."[29] The final considerations in the risk assessment draw on past compliance history and other information that affect reasons for potential concern.

This regime offers establishments' flexibility in how they develop and implement their PCPs. But oversight is still retained by CFIA, and the agency's ability to efficiently prioritize inspection efforts. In theory, this oversight should be improved given the greater information available on establishments that comes from the wider and more consistently applied licencing requirements.

A. Time and Money Barriers to Entry

The Canadian government was aware of the potential concerns about the compliance costs of the SFCA and the associated regulations. The CFIA's (2017) *Regulatory Impact Analysis* noted that costs of the new requirements, particularly the development and implementation of PCPs, would mostly be borne by small businesses; this was because larger businesses would already have a PCP-like plan in place.[30] From 2017 to 2027, this analysis estimated that small businesses would produce 13,915 new PCPs, whereas medium and larger businesses would only produce 39. These expectations are consistent with findings from other jurisdictions that highlight how food safety requirements can create heavier burdens on smaller businesses (Adalja & Lichtenberg, 2018) and do not capture the full extent of barriers to entry, particularly those that occur within provinces and territories due to other licencing requirements (Berger Richardson, 2020).

Private-sector efforts have sought to address these concerns, to an extent. For instance, GFSI formed to deal with, among other issues, the duplication of audits, which were partly creating barriers to entry by forcing suppliers to undertake

[29] https://inspection.canada.ca/about-cfia/transparency/consultations-and-engagement/completed/regulatory-risk-based-oversight/private-certification-policy/eng/1452808755126/1452808821799?chap=0
[30] https://www.gazette.gc.ca/rp-pr/p1/2017/2017-01-21/html/reg1-eng.html

multiple different audits to meet different buyer's expectations. Follow up surveys, however, have shown that audit duplications continue to be an issue (Crandall et al., 2017).

B. Oversight Mechanisms to Ensure Trained and Continued Auditor Competence

Training of qualified professionals for food safety is a shared activity, taken on by the Canadian industry and governments. On the industry side, third-party audit firms have developed extensive training programs designed for food sector employees involved in meeting private and public food safety requirements. Examples included Intertek's Alchemy and SGS's various training programs specific to industry food safety standards like FSSC 22000. On the government side, professional credentials are, in certain provinces and municipalities, a requirement for licenced food establishments. Alberta, for instance, requires that food establishments hire staff that have completed a *Food Handler Certification*, offered by the Canadian Institute of Food Safety. In Manitoba, it is only establishments in Winnipeg that require this certification of staff.

C. Balancing Market Efficiency and Third-Party Auditing's Race-to-the-Bottom Nature

The focus on third-party audits as one factor in the establishment-based risk assessment model developed by CFIA to direct inspection efforts suggests little effort to steer or shape the nature of these audits. As noted above, CFIA has several guidance documents that illustrate how a quality management and HACCP approach can be used to develop a PCP; these guidance documents make clear that there are many acceptable approaches to a PCP. No explicit mention is made of how third-party audits ought to be conducted, which leaves harmonization and standard setting to the private sector such as through the GFSI mentioned above (Gerardi, 2023).

D. Public Regulators Creating Favourable Conditions to Raise Auditing Standards

The approach taken in the current Canadian regime would appear to have little influence on audit standards, beyond the establishment of baseline requirement that licenced establishments must prepare a PCP. Reports from industry suggest that voluntary requirements, such as those of benchmarked standards recognized by the GFSI, create higher expectations that legal requirements (Fulponi, 2006). But

the choice of how harmonization occurs and what potential increases in these standards might be in the future are left to private actors. Indeed, the benchmarking requirements focus both on the substance of the food safety standards as well as the compliance procedures used by third-party auditors for those schemes (Havinga & Verbruggen, 2017).

4. Canada's Data Governance and Data Privacy Audit Approach

Independent of, but related to AI-specific efforts, and like the GDPR and *Digital Services Act*, there are Canadian efforts to deal with data governance and data privacy that touch on similar roles for auditors as the EU case. Canadian privacy, and, by extension, data privacy, is legislated under the *Personal Information Protection and Electronic Documents Act* (PIPIDA), which covers how businesses handle personal information, and the *Privacy Act*, which covers how the federal government handles personal information. Both *Acts* are enforced by The Office of the Privacy Commissioner of Canada (OPCC) and, while not explicitly stated, cover Canada's data governance efforts. Bill C-27 may change that if passed with its proposed *Consumer Privacy Protection Act* (CPPA) and *Personal Information and Data Protection Tribunal Act* (PIDPTA). These new laws would shift the current legislative language around privacy and data governance and add an additional oversight body. While these Canadian data privacy and data governance efforts are useful, they all miss out on the role of auditors, with only PIPEDA (Section 18) and CPPA (Sections 97, 98, and 99) including language, albeit vague, around auditors' role in data privacy and data governance.

Despite auditors' unclear role, Canadian data privacy and data governance audits occur by qualified auditors across the public and private sector as both are expected to be able to demonstrate their compliance with their governing *Act*. Under PIPEDA's *10 Fair Principles*, businesses are required to complete OPCC's Privacy Impact Assessments (PIAs) that demonstrate that businesses' compliance with PIPEDA's *10 Fair Principles.* PIAs are completed when businesses decide to introduce a new policy or service that collects consumer data; begin a relationship with the Federal government; or intend to transfer their collected client data cross-border, among other criteria. These private-sector PIAs are conducted internally or externally by auditors. Similarly, PIAs are required for government agencies, departments, or institutions under the Treasury Board Secretariate's Directive on Privacy Impact Assessments despite the *Privacy Act* containing no audit-related

language. These government PIAs are conducted internally by the same department, agency, or institution needing the audit (e.g., the Privy Council Office will have their own audit team audit themselves).

A. Time and Money Barriers to Entry

Internal federal government agency, department, and institutions' data privacy or data governance audit timelines are not publicly available, but presumably vary depending on audit team workload, sufficient data privacy and data governance competence, and cooperation with those requesting the audit. These internal government audits are effectively free as they are conducted internally (presenting no money barrier), only costing the internal audit team's time. As for the third-party auditor's PIA completion timeline and costs, both are unknown in the current academic literature and across the big four auditing firms' websites. Despite this lack of third-party auditor PIA timeline and cost information, private-sector firms can engage the OPCC to help them complete PIAs or use their *PIPEDA Self-Assessment Tool* to assess their compliance and develop appropriate privacy frameworks when needed. While these efforts might take more time than going through a third-party auditing firm, the OPCC provides this service for free. These efforts reduce the money barrier to entry for all public institutions and private firms, thereby providing a near even playing field for data privacy and data governance compliance within Canadian small, medium, and large firms, and government institutions (Wright, 2012). More information is needed to determine the time-related barrier to entry as neither public nor third-party audit timelines are public.

B. Oversight Mechanisms to Ensure Trained and Continued Auditor Competence

Oversight mechanisms used to ensure trained and continued data privacy and data governance auditor competence is left up to industry associations like the IAPP, Data Management Association (DAMA), Information Systems Audit and Control Association (ISACA), and International Information System Security Certification Consortium (ISC2) that each offer various data privacy and data governance-related professional certifications. IAPP offers the CIPP– Canada, Certified Information Privacy Manager, and Certified Information Privacy Technologist certifications and their previously mentioned soon to be released

AIGP certification in the first few months of 2024.[31] DAMA offers the Certified Data Management Professional certificate;[32] ISACA offers the Certified Information Systems Auditor certificate;[33] and ISC2 offers the Certified Information Systems Security Professional certificate.[34] Each of these certifications require annual training, usually on current and emerging data privacy and data governance content, to maintain the certifications and ensure continued competence.

While these professional certifications cover slightly different content, they are sought after when hiring data privacy and data governance auditors in the public and private sector as they ensure, or are at least the best indicator, that an applicant and potential auditor will be familiar with the current state of the Canadian data privacy and data governance legislation, regulation, policy, various auditing criteria and how to assess against them, etc. and will be required to update their knowledge annually to maintain their certification(s).

C. Balancing Market Efficiency and Third-Party Auditing's Race-to-the-Bottom Nature

Since the OPCC's PIA requirement of the Canadian public and private sector and set criteria of what's included in those PIAs, the race-to-the-bottom nature of third-party auditing is far less pronounced than other cases, such as the EU's potential race-to-the-bottom in data protection auditing. The only possible race-to-the-bottom will be third-party auditors' PIA service price as PIA criteria cannot be changed by the third-party auditors. This limit to service price changes will create a theoretical price floor for third-party auditors conducting PIAs and other similar data privacy and data governance audits. Prices will increase as some third-party audit firms gather more expertise than others (such as hiring auditors with one or more of the professional certifications above), offer faster and more efficient PIAs, and gain a positive reputation for their PIA outcomes.

[31] https://iapp.org/certify/
[32] https://cdmp.info/about/
[33] https://www.isaca.org/credentialing/cisa
[34] https://www.isc2.org/certifications/cissp

D. Public Regulators Creating Favourable Conditions to Raise Auditing Standards

The usual Canadian third-party auditors, like the big four auditing firms, have a minimal role to play in the Canadian data privacy and data governance auditing regimes. These firms only carry out OPCC's PIAs. Rather than large auditing firms competing and setting their own internal data privacy and data governance auditing requirements, the OPCC does so. The OPCC does this through their enforcement of both *PIPEDA* and the *Privacy Act*, setting and updating the criteria of these *Acts* required PIAs, and having the power to audit any private firm or public institution when they have reasonable grounds to believe they are contravening either *Act*, usually when there are recuring complaints against a particular firm or institution, or if they routinely perform poorly on PIAs (Toy & Hay, 2015). The OPCC's power to set auditing standards through their PIA criteria and audit those contravening their Acts or poorly performing on PIAs creates favourable conditions to maintain stable and consistent auditing standards. Such stable and consistent audit standards set an expectation for third-party audit firms and their clients, setting a sort of auditing standards floor. While the OPCC does not continuously raise auditing standards, they do set this auditing standards floor, thereby raising auditing standards initially and avoiding the race-to-the-bottom issue appearing in other cases.

Case Discussion and Workshop Insights

This section discusses the overarching insights from the collection of case studies and the workshop that took place on November 9th, 2023, with participation from academic, industry, and civil society leaders working in AI, auditing, and AI auditing. During this workshop, we explored each of this paper's four themes and how they are currently emerging in the AI audit field and how they might be informed from other industries' auditing efforts. In addition to exploring these themes, the workshop participants raised several unanswered questions, concerns, and opportunities they have experienced in their varied roles. This section is divided into the paper's four themes with each theme's subsection outlining the overarching insights from the case studies and how that theme was discussed in the workshop in relation to AI auditing.

A. Time and Money Barriers to Entry

Each of the cases highlighted the potential for barriers occurring due to the requirements for audits to assess potential risks or regulatory compliance issues. These challenges were often understood by legislators and regulators. For instance, the SFCA detailed the specific burdens that the new requirements for developing and implementing PCPs would create for small and medium businesses in the food sector. Different measures devised to offset these challenges were also apparent in the cases, such as simplified calculation methodologies and group audit processes for biofuels and free assessments for data privacy in Canada. These cases make clear that it is important to understand the nature of barriers created by audit expectations to discern whether reasons for not being able to meet audit requirements are due to the targeted risks of harm or due to capacity or resource constraints to simply document and report the absence of those harms. Regulators ought to seek ways to ensure audits do not serve to push safe AI systems off the market due merely to the cost of conducting the audit.

The workshop participants expanded on these case study insights. A recurring theme of the discussion was how the current state of AI audits is preventing firms from meaningfully engaging in the space. For instance, some audit firms are declining opportunities to conduct AI audits when their clients request them or are taking an extended time to complete these audits. Several reasons for these refusals and delays were discussed.

First, there is the continued challenge that the object of the AI audit remains unclear. Is it the AI system; the data used within the AI system; the organization's internal policies for how the AI system or its data are used and managed; the organization's compliance with existing and future laws and regulations (like the EU AI Act and Canada's AIDA)? Equally, questions were raised about whether audits should use product, process, technical, or management system international standards to audit against (like ISO 42001, 17065, or 23894); or some combination of these or something else entirely?

Second, thresholds for acceptability remain unclear. It is difficult to determine when the object of the AI audit is "good enough" to pass the AI audit. Does it pass

at 50%, 60%, 70%, 71%, or some other threshold against some expectations of potential impacts and harms?

Third, and related to the next theme, the discussion raised issues about the lack of qualified and credentialled AI auditors which can contribute to making these services more costly and protracted to undertake. These service time and cost barrier are occurring because firms are competing for limited talent, thereby potentially raising the price of AI audits, and increasing how long it takes firms to complete these AI audits when they lose the talent competition.

B. Oversight Mechanisms to Ensure Trained and Continued Auditor Competence

Consistent with the previous points, the existence of competent audit organizations and auditors cannot be taken for granted, particularly on an emerging risk like AI. Several of the case studies highlighted the extensive and ongoing efforts needed to ensure a continued supply of professionals capable of auditing against the requirements of biofuel, privacy, and food safety standards.

Industry associations, private standard-setters, and audit organizations play a large role in credentialling their industry professionals against various bodies of knowledge, such as IAPP and the EU GDPR Institute. But, legislative and regulatory efforts can also include provisions around ensuring organizations are demonstrating their competence in a particular area through audit or under threat of public auditing. The EU's efforts to raise standards on training of competent auditors in the renewable biofuels case highlights how this can be a valuable area for regulatory oversight, particularly as these expectations have been refined and expanded with time and through learning. Ensuring there is sufficient transparency about the experiences of auditing in the initial phase of AI regulation appears critical for ensuring training expectations can be continually improved.

This theme was the most contentious and discussed throughout the workshop. Participants introduced differing perspectives on oversight mechanisms and how to ensure competence of AI audits and auditors.

First, professional credentialling was considered important and likely to take multiple forms. For instance, organizations like the Institute of Internal Auditors, which offers a professional credential for internal auditors could extend this to

create an AI audit professional credential for internal AI auditors, while leaving general AI governance professionals, such as management and executive positions to other professional credentialing efforts like the IAPP's AIGP, which includes general AI audit information in their testing materials and Body of Knowledge.

Second, and largely uncontested, was the need to recognize international credentials to build national capacity. Given the lack of global competence to carry out and provide AI audits, even computer scientists cannot consistently verify their AI systems on a technical level, finding ways to recognize and verify international AI auditing credentials is key to reducing the barrier and money barriers discussed earlier.

Third, the question was raised as to whether AI developers should become a licensed profession (like lawyers, doctors, accountants, and social workers, etc.) given the power, knowledge, and influence they have over their created AI systems, and, by extension, those who use these AI systems. The issues with this question are like the other credentialling-related concerns. Who offers this license? How is it compared across jurisdictions? Why would AI developers want to become licensed? What incentives could be offered to get AI developers to seek licensure?

C. *Balancing Market Efficiency and Third-Party Auditing's Race-to-the-Bottom Nature*

The cases all illustrated that an awareness of the trade-offs and tensions between efficiency and some level of consistency and quality are important considerations for public regulators that delegate oversight to third-party audit organizations. Depending on how many third-party auditors there are in each market will influence their market efficiency vs. race-to-the-bottom nature. Markets with many third-party auditors will be forced to compete, producing a race-to-the-bottom in cases where public regulators have not created an audit requirement floor or incentives to offer increased audit standards.

During the workshop, those with previous regulatory experience were quick to point out the risks of implementing stringent rules to reduce the race-to-the-bottom issue and improve market efficiency. Sometimes, if stringent rules are implemented too quickly, especially as a market emerges, it may lead to industry

push back, poor compliance, and smaller firms being priced or pushed out of the market for being unable to comply with these rules, benefitting larger firms with larger compliance budgets and capacity. While these rules are often touted to reduce the race-to-the-bottom nature of rule avoidance, they can have unintended consequences that reduce market efficiency. Similarly, determining which AI systems should be audited could improve market efficiency rather than the current state of AI auditing that is unclear on which AI systems should be audited, when in the AI system lifecycle, by what criteria, and by whom.

Conversely, some participants argued that these questions are less important to figure out in the short-term over simply "doing something." Arguing that doing something now and then improving and iterating on it will meet the current market demand for AI auditing services rather than doing nothing. However, this doing something approach ignores the potential quality/rigour issues that emerge from less stringent rules being implemented, allowing for an environment that promotes race-to-the-bottom behaviour. This exact chain of events was experienced by early AI system and organizational control assessments and audits against those assessments. A few early players in the AI assessment and audit field took the "doing something" approach improved and iterated on their assessments and audit practices as they gained more clients. The race-to-the-bottom was seemingly avoided as there were only a handful of firms offering these services and they each focused on a different aspect of AI system's, such as product, data, bias, and management practices. Lastly, it was debated whether the EU *AI Act* was becoming the benchmark for AI rules, creating an almost regulatory floor for firms to comply with and other legislative and regulatory efforts to mimic.

D. Public Regulators Creating Favourable Conditions to Raise Auditing Standards

Public regulators take a few different approaches when creating conditions favourable to raising auditing standards. First, they can include or reference a set of guiding principles that audits should audit against, as seen in Canada's data privacy case. Second, they can require that organizations complete assessments without including any language on what that assessment should contain, like the Canadian food inspection regime. Third, they can do nothing and leave audit standards up to industry, like the EU data protection case.

This theme was the least discussed at the workshop because time was limited and more time was spent on the other themes, and it is the least developed of the four themes as Canada's AIDA is being revised for the next legislative step. While limited, three general ideas were discussed around this theme. First, it was brought up throughout the workshop that since AI systems are often dynamic in nature, finding a consistent way to assess and audit them becomes difficult. This difficultly may be addressed through a series of focused and coordinated international standards, such as product, process, management system, or technical standards, and public regulatory efforts, or collaboration of both. Second, Canadian public regulators, particularly Innovation, Science, and Economic Development, should work towards creating baseline AI audit requirements, criteria, or principles, must like the OPCC did with PIPEDA's *10 Fair Principles*. Third, workshop participants brought up the differences in political will between the EU, Canada, and the US related to their AI regulatory approaches, evidenced by differences in the EU *AI Act*, Canada's *AIDA*, and recently released US *Executive Order on the Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*.

Conclusion: Emerging Themes and Future Research Questions

Our cross-case comparison and workshop insights highlight several considerations relevant to how third-party audits might be used in the context of AI regulation in relation to our guiding questions. To conclude, we (A) detail four themes that emerged across the case discussion and workshop insights and (B) outline outstanding questions for future research.

A. Emerging Themes

Through the cases reviewed, three additional themes emerged. First, audits may serve more than one function, and early in the development of a new regulatory approach, information provisions may be particularly important. Consider the SFCA example. In that case, CFIA viewed the new licencing regime as an opportunity to build a deeper understanding of the food establishments under its oversight. Requirements to disclose key information may help ensure future refinements to the regulatory approach, and it may, if done well, offset the potential information asymmetries that will give businesses generating new AI systems an inherent advantage in understanding and strategically pushing for certain forms of regulatory oversight (Perlman, 2023). Current work suggests that

transparency of leading AI firms is far short of what would be optimal from a public policy perspective.[35] Thus, a transparency role for audits seems highly relevant and worthy of consideration.

Thinking about ways to overcome information asymmetries in the short run may additionally reveal further possibilities for how audits can work alongside other compliance incentives that may exist for AI system developers. Reputational concerns, learning, peer and network effects, liability, and social pressure can at times and in specific circumstances serve to complement regulatory compliance incentives. Structuring audit requirements to enhance and deepen these incentives, rather than crowd them out, appears a useful path for future consideration.

Second, it is important not to assume that AI audit capacity exists in Canada, especially given its required specialized knowledge, limited ways to demonstrate that knowledge (for those that have it) as few professional certification programs are established, and an already tight competition to attract those with this knowledge. This capacity gap may need to be actively supported and developed by governments. This is true for the organizations that run the audits, and for the individual auditors that do the specific audit assessments. Different questions of training and oversight apply depending on whether we are considering individuals or organizations.

Third, regulatory bodies need to be aware of, and prepared to steer the way in which audit markets operate. This is equally true for the audit organizations and the individual auditors. Canadian regulatory bodies do not have the knowledge capacity to regulate AI, let alone steer the AI audit market, balance market efficiency and the race-to-the-bottom, and create favourable conditions to raise Canadian AI audit standards.

Lastly, the workshop participants raised several recommendations stemming from one recurring issue: to determine what the object of AI audits is/should be. AIDA should aim to include some required audit criteria in their forthcoming regulations to set an AI auditing floor. These required criteria do not need to be comprehensive or overly detailed, just some general required criteria that cover the AI systems. Third, Canadian regulators, audit firms, and auditors should strive to

[35] https://hai.stanford.edu/news/introducing-foundation-model-transparency-index

create a system where the audit result is valuable for both the audited entity and the public. This recommendation would require definition and clarity on audit standards and expectations for their purpose/outcomes and to provide public transparency around audit quality (such as making it difficulty for the auditor to cut corners, avoiding the race-to-the-bottom to generate business) to avoid reputational risk/brand credibility harm. Lastly, it is better to so something imperfect now than continue doing nothing at all given the market and regulatory demand for AI auditing services.

B. Future Research Questions

1. How should ongoing AI auditing efforts address these barriers to entry and what should regulators consider in future regulatory and legislative efforts given the emerging third-party AI audit industry?

2. Should AIDA include provisions around auditor and organizational competence around AI? And if so, how? Should they require accredited professional designations to complete AI audits?

3. As the big four audit firms and smaller boutique audit firms build their AI audit competencies and more Canadian organizations, including government, incorporate AI into their business and operations, how should Canadian audit firms and public regulators prepare for the likely race-to-the-bottom given the lack of public regulations around AI audits in AIDA?

4. In what ways should AIDA's forthcoming regulations address the role of auditors? Should they clearly define all aspects of audits and auditor's role? Or only require that organizations complete audits? Similarly, should regulators include a list of guiding principles that audits ought to audit against, like Canada's data privacy case. Maybe ISED's recently released *Voluntary Code of Conduct on the Responsible Development and Management of Advanced Generative AI Systems'* principles' could serve as these audit's guiding principles much like PIPEDA's *10 Fair Principles* do for Canadian privacy audits.

5. What is the object of the AI audit? This question was recurring throughout the workshop, being brought up across all themes.

6. Do oversight mechanisms have varied success in micro vs. macro efforts? Some oversight mechanisms may be better suited for sector/industry-specific governance efforts while others may be better suited for general governance efforts. This question should be explored in relation to sector/industry-specific or general AI audits.

7. Some of the terms are understood differently between different actors. Discuss examples of these (audit, verification, certification, assessment, assurance, etc.) and what the implications of these different understanding may mean, including how they work and why they do and do not work.

8. Property rights vs. open source. Who holds responsibility? What are the rules for open source and the implications of them? Possible parallel to public vs. private financial reporting.

References

Adalja, A., & Lichtenberg, E. (2018). Produce growers' cost of complying with the Food Safety Modernization Act. *Food policy*, *74*, 23-38. https://doi.org/https://doi.org/10.1016/j.foodpol.2017.10.005

Auld, G., Casovan, A., Clarke, A., & Faveri, B. (2022). Governing AI through ethical standards: Learning from the experiences of other private governance initiatives. *Journal of European Public Policy*, *29*(11), 1822–1844. https://doi.org/10.1080/13501763.2022.2099449

Auld, G., Gulbrandsen, L. H., & McDermott, C. L. (2008). Certification schemes and the impacts on forests and forestry. *Annual review of environment and resources*, *33*, 187-211.

Auld, G., & Renckens, S. (2023). *Qualities of Market Assurances: Individuals as Regulatory Intermediaries in Seafood Sustainability Audits* [Working Paper].

Berger Richardson, S. (2020). *Is safe food good food? Looking beyond safety to regulate good food systems* McGill University].

Bishop, K., & Carlson, K. (2022). The role of third-party audits in ensuring producer compliance with the Roundtable on Sustainable Palm Oil (RSPO) certification system. *Environmental Research Letters*, *17*(9), 094038.

Büthe, T., & Mattli, W. (2011). *The new global rulers: The privatization of regulation in the world economy*. Princeton University Press.

Champagne, F.-P. (2023). *ISED's Letter to the Standing Committee on Industry and Technology House of Commons on AIDA's Amendments*. https://www.ourcommons.ca/content/Committee/441/INDU/WebDoc/WD12751351/12751351/MinisterOfInnovationScienceAndIndustry-2023-11-28-Combined-e.pdf

Charlebois, S., Juhasz, M., Music, J., & Vézeau, J. (2021). A review of Canadian and international food safety systems: Issues and recommendations for the future. *Comprehensive Reviews in Food Science and Food Safety*, *20*(5), 5043-5066. https://doi.org/https://doi.org/10.1111/1541-4337.12816

Crandall, P. G., Mauromoustakos, A., O'Bryan, C. A., Thompson, K. C., Yiannas, F., Bridges, K., & Francois, C. (2017). Impact of the Global Food Safety Initiative on Food Safety Worldwide: Statistical Analysis of a Survey of International Food Processors. *Journal of Food Protection*, *80*(10), 1613-1622. https://doi.org/https://doi.org/10.4315/0362-028X.JFP-16-481

Fulponi, L. (2006). Private voluntary standards in the food system: The perspective of major food retailers in OECD countries. *Food policy*, *31*(1), 1-13.

Gerardi, A. (2023). Chapter 70 - Global Food Safety Initiative (GFSI): underpinning the safety of the global food chain, facilitating regulatory compliance, trade, and consumer trust. In M. E. Knowles, L. E. Anelich, A. R. Boobis, & B. Popping (Eds.), *Present Knowledge in Food Safety* (pp. 1089-1098). Academic Press. https://doi.org/https://doi.org/10.1016/B978-0-12-819470-6.00058-5

Havinga, T., & Verbruggen, P. (2017). Understanding complex governance relationships in food safety regulation: The RIT model as a theoretical lens. *The Annals of the American Academy of Political and Social Science*, *670*(1), 58-77.

Jobin, A., Ienca, M., & Vayena, E. (2019). The global landscape of AI ethics guidelines. *Nature Machine Intelligence*, *1*(9), 389-399. https://doi.org/10.1038/s42256-019-0088-2

Loconto, A., & Busch, L. (2010). Standards, techno-economic networks, and playing fields: Performing the global market economy. *Review of international political economy*, *17*(3), 507-536.

Michaelowa, A., & Jotzo, F. (2005). Transaction costs, institutional rigidities and the size of the clean development mechanism. *Energy Policy*, *33*(4), 511-523.

OECD. (2022). *National AI policies & strategies*. https://oecd.ai/en/dashboards

Peltzman, S. (1976). Toward a more general theory of regulation. *The Journal of Law and Economics*, *19*(2), 211-240.

Perlman, R. L. (2023). *Regulating Risk: How Private Information Shapes Global Safety Standards*. Cambridge University Press.

Ponte, S. (2008). Greener than thou: The political economy of fish ecolabeling and its local manifestations in South Africa. *World Development*, *36*(1), 159-175. https://doi.org/DOI 10.1016/j.worlddev.2007.02.014

Power, M. (1997). *The audit society: Rituals of verification*. Oxford University Press.

Renckens, S. (2020). *Private Governance and Public Authority. Regulating Sustainability in a Global Economy*. Cambridge University Press.

Renckens, S., & Auld, G. (2022). Time to certify: Explaining varying efficiency of private regulatory audits. *Regulation & Governance*, *16*(2), 500-518. https://doi.org/https://doi.org/10.1111/rego.12362

Sabel, C. F., & Zeitlin, J. (2008). Learning from difference: The new architecture of experimentalist governance in the EU. *European Law Journal*, *14*(3), 271-327.

Saes, B. M., & Muradian, R. (2021). What misguides environmental risk perceptions in corporations? Explaining the failure of Vale to prevent the two largest mining disasters in Brazil. *Resources Policy*, *72*, 102022. https://doi.org/https://doi.org/10.1016/j.resourpol.2021.102022

Short, J. L., Toffel, M. W., & Hugill, A. R. (2016). Monitoring global supply chains. *Strategic Management Journal*, *37*(9), 1878-1897.

Sinclair, T. J. (2014). *The new masters of capital: American bond rating agencies and the politics of creditworthiness*. Cornell University Press.

Skogstad, G. (2008). *Internationalization and Canadian agriculture: Policy and governing paradigms* (Vol. 30). University of Toronto Press.

Stigler, G. J. (1971). The Theory of Economic Regulation. *The Bell Journal of Economics and Management Science*, *2*(1), 3-21. https://doi.org/10.2307/3003160

Toffel, M. W., Short, J. L., & Ouellet, M. (2015). Codes in context: How states, markets, and civil society shape adherence to global labor standards. *Regulation & Governance*, *9*(3), 205-223. https://doi.org/10.1111/rego.12076

Toy, A., & Hay, D. C. (2015). Privacy Auditing Standards. *Auditing: A Journal of Practice & Theory*, *34*(3), 181-199. https://doi.org/10.2308/ajpt-50932

Verbruggen, P. (2022). Tort Liability of Private Safety Auditors in Global Value Chains. *European Journal of Risk Regulation*, *13*(4), 584-602. https://doi.org/10.1017/err.2022.29

Wright, D. (2012). The state of the art in privacy impact assessment. *Computer Law & Security Review*, *28*(1), 54-61. https://doi.org/10.1016/j.clsr.2011.11.007