ONTARIO ENERGY BOARD

IN THE MATTER OF subsections 74(1)(b), 78(2.1), (3), (3.0.1), (3.0.2) and (3.0.3) of the *Ontario Energy Board Act, 1998*;

AND IN THE MATTER OF subsections 53.8 of the *Electricity Act, 1998*;

AND IN THE MATTER OF Ontario Regulation 453/06 made under the *Ontario Energy Board Act, 1998*;

AND IN THE MATTER OF an Application by the Independent Electricity System Operator (the "**IESO**"), designated as the Smart Metering Entity (the "**SME**"), to approve fees for providing third party access to smart meter data;

AND IN THE MATTER OF an Application by the IESO, designated as the SME, to amend section 6.1 of the Smart Metering Entity Licence ES-2021-0191 (the "**SME Licence**").

APPLICATION

1. The applicant, the IESO, is a corporation without share capital continued under Part II of the *Electricity Act, 1998* (the "**Electricity Act**"), which is designated as the SME by Ontario Regulation 393/07 made under the Electricity Act and is the holder of the SME Licence issued September 2, 2021.

2. The objects of the SME under the Electricity Act and Ontario Regulation 393/07 include, but are not limited to, collecting and managing specified information and data related to the metering of electricity in Ontario and providing and promoting non-discriminatory access by distributors, retailers, the IESO and other persons to this information and data (referred to as "**Third Party Access**" or "**TPA**").

3. On March 24, 2022, the Ontario Energy Board (the "**OEB**") approved the SME's application (EB-2021-0292), which included a framework to provide TPA of de-identified smart metering data to "**Canadian Governmental Entities**"[1] and a charge for both

[1] "**Canadian Governmental Entities**" is defined in the OEB decision and order EB-2021-0292 (the "**Decision and Order**") as federal and provincial governments, including ministries, agencies, boards, commissions, tribunals and wholly-owned corporations, or in the case of non-share capital corporations, where such corporations are controlled by a federal or provincial governments, as well as municipalities (or regional governments), universities, school boards, hospitals and First Nations. First Nations means a "council of the band" as defined in subsection 2(1) of the *Indian Act* (Canada). Canadian Governmental Entities does not include private sector entities, publicly traded companies, individual doctors, professors, or government officials and all those entities that do not fall in one of the

standard and non-standard requests at a fee of $145/hour, with the exception of requests made by the IESO or the OEB which are fulfilled at no charge. In the Decision and Order, the OEB approved a settlement proposal under which the SME agreed to undertake an assessment of the benefits of expanding TPA beyond Canadian Governmental Entities by April 30, 2025.

4. On December 16, 2024, the SME submitted a report titled "Assessment of Expanding Third Party Access to SME Data Beyond Currently Approved Parties" to the OEB and provided a copy to all intervenors in EB-2021-0292 (the "**TPA Assessment Report**"). In the TPA Assessment Report, the SME concluded:

   (a) there is strong market interest in smart metering data and expanding TPA beyond Canadian Governmental Entities would provide benefits to both SME ratepayers and energy sector participants; and

   (b) expanding TPA to smart metering data is unlikely to create any incremental risks to consumers, local distribution companies ("**LDCs**"), the SME or the IESO.

5. Effective July 1, 2023, Ontario Regulation 133/23 amended Ontario Regulation 393/07 to expand the SME's mandate. The regulation added new objects authorizing the SME to:

   (a) collect, manage and store information and data related to the metering of electricity that is conveyed into a distributor's distribution system, including data collected from distributors; and

   (b) provide and promote non-discriminatory access, on appropriate terms and subject to any conditions in the SME Licence relating to the protection of privacy, to information and data related to the metering of electricity that is conveyed into a distributor's distribution system.

6. The effect of these new objects is to broaden the SME's statutory authority beyond consumption data to include generation data (e.g., from behind-the-meter distributed energy resources such as rooftop solar), reflecting the evolving nature of Ontario's electricity system and the increasing role of prosumers.

7. For the purposes of this application, the term "**SME data**" refers to any of the data and

---

categories outlined above.

information related to the metering of consumers' electricity consumption or usage in Ontario (including the data collected pursuant to the OEB's direction in EB-2016-0284), and any data and information related to the metering of electricity that is conveyed into a distributor's distribution system, including data collected from distributors.

8. The SME is now seeking the OEB's approval to:

   (a) charge a fee of $145/hour on a cost recovery basis to provide TPA to de-identified SME data to "**Canadian-Status Non-Governmental Entities**"[2] and to other entities when such access is required to support government or OEB directed initiatives and activities; and

   (b) amend section 6.1 of the SME Licence to enable the SME to provide and promote non-discriminatory access on appropriate terms and subject to any conditions in the SME Licence relating to the protection of privacy, information and data related to the metering of electricity that is conveyed into a distributor's distribution system.

9. The SME has filed evidence in support of this application as identified in the Exhibit List, Ex A-2-1. The SME may amend its pre-filed evidence from time to time prior to, and during, the course of the OEB's proceeding. In particular, should the SME identify a material change to its application, the SME will advise the OEB and update its pre-filed evidence. The SME reserves the right to amend its application, accordingly, including making any necessary adjustments to the approvals sought in this application.

10. The SME respectfully requests that the OEB dispose of this application without a hearing, pursuant to paragraph 21(4)(b) of the *Ontario Energy Board Act, 1998*, as no other person will be adversely affected in a material way by the outcome of the proceeding; in particular:

   (a) The proposed expansion of TPA is consistent with prior OEB decisions and directions and does not result in any adverse impacts on ratepayers or market participants.

   (b) The proposed expansion represents the logical next step in the SME's measured

[2] "**Canadian Status Non-Governmental Entities**" means the requestor, and where relevant, the ultimate controlling parent entity, who have attested (through an authorized representative of each of the respective parties) to having their main office or headquarters located in Canada.

and transparent approach to expanding TPA access, prioritizing privacy protections, cost-effectiveness, and alignment with the public interest.

(c) The SME's proposed TPA expansion does not change the risk profile, or create incremental risks to consumers, LDCs, the SME or the IESO.

(d) The SME will continue to provide TPA to SME data in accordance with the framework detailed in EB-2021-0292, including, but not limited to, the Ethics Committee and the Data Use Agreement (the "**DUA**") and will continue to assess its data protection methods to be responsive to changes in applicable legislation and best practice.

(e) The requested licence amendment will create consistency between the TPA framework and the SME's legislative authority.

11. The SME further notes that no questions or comments were received from OEB staff or intervenors in response to the TPA Assessment Report filed with the OEB.

12. The SME requests that all documents issued by the OEB, and, if a hearing is held, all filings submitted to the OEB by parties to this proceeding, be served on both the SME and its legal counsel as follows:

(a) the SME:

Mr. Phillip Chisulo
Senior Advisor, Regulatory Affairs
Independent Electricity System Operator

Mailing address:
120 Adelaide Street West, Suite 1600
Toronto, Ontario, M5H 1T1

Tel: +1 416 969 6045
E-mail: regulatoryaffairs@ieso.ca

(b) the SME's counsel:

Mr. Patrick G. Duffy
Stikeman Elliott LLP

Mailing address:
5300 Commerce Court West, 199 Bay Street
Toronto, Ontario, M5L 1B9

Tel: +1 416 869 5257
E-mail: pduffy@stikeman.com

DATED at Toronto, Ontario, this 7th day of November 2025.

INDEPENDENT ELECTRICITY SYSTEM OPERATOR

By its counsel in this proceeding
Patrick G. Duffy

SMART METERING ENTITY
EXPANDING THIRD PARTYACCESS
(EB-2025-0272)

EXHIBIT LIST

Exhibit	Tab	Schedule	Description
A – ADMINISTRATION			
A	**1**	**1**	Application
A	**2**	**1**	Exhibit List
B – SUPPORTING EVIDENCE			
B	**1**	**1**	Expanded Third Party Access Framework
B	**1**	**2**	Smart Metering Entity, Assessment of Expanding Third Party Access to SME Data Beyond Currently Approved Parties
B	**1**	**3**	Accenture Inc., Assessment of Risks & Opportunities with Expanding Third Party Access to Smart Metering Entity Data
B	**1**	**4**	Privacy Analytics, AI Threats and Risk Implications, AI Risk Tiering for Anonymized Electricity Consumption Data
B	**2**	**1**	Cost Recovery Model for Third Party Access
B	**3**	**1**	Terms of Access Principles

EXPANDED THIRD-PARTY ACCESS FRAMEWORK

1. To meet the OEB's directive in EB-2021-0292, and its request that the SME "consider expediting its assessment of expanding access to Meter Data Management Repository (MDM/R) data to entities beyond Canadian Governmental Entities sooner than 2025"[3], the SME submitted the TPA Assessment Report evaluating the expansion of TPA on December 16, 2024.

2. The TPA Assessment Report was informed by two key external assessments conducted by Accenture Inc. ("**Accenture**") and Privacy Analytics Inc. ("**PA**"), whose expertise was critical in evaluating both the benefits and risks of expanding TPA.

3. Accenture was engaged to lead the risk and opportunity assessment component of the study. Accenture undertook a comprehensive assessment of the risks associated with expanding TPA access to SME data, focusing on three key areas: (i) grid security, (ii) market manipulation, and (iii) de-anonymization. This assessment drew on a range of resources, including global power and utilities industry specialists, artificial intelligence (AI) and generative artificial intelligence ("**AI**") advisors, and dedicated research teams.

4. Following its investigation, Accenture delivered a report entitled *Assessment of Risks & Opportunities with Expanding Third Party Access to Smart Metering Entity Data* dated September 23, 2024. In its assessment, Accenture found that incremental risk across each of the respective three areas was unlikely to occur:

> [E]xpanding TPA to SME data beyond Canadian Governmental Entities does not appear to result in any scenarios that would likely increase the existing overall risk profile of the IESO or SME. Rather, it appears that the expansion of TPA to SME data would yield many positive opportunities in the market that may benefit Ontario ratepayers.

5. PA was retained to conduct privacy and data security assessments with particular focus on implications of AI and potential data re-identification. PA's analysis, *AI Threats and Risk Implications, AI Risk Tiering for Anonymized Electricity Consumption Data*, focused on assessing the effectiveness of the SME's current data security and privacy protections

[3] EB-2021-0292 OEB Decision and Order, March 24, 2022.

in defending SME data against growing AI threats. Based on its assessment, PA assigned the SME an “AI Risk Determination” score of “Low”, stating “given the de-identification methods employed by the IESO SME to manage risks from sharing aggregated data. The risk of AI systems using this data is low.”

6. Four tiers of AI Risk Determination exist: Low, Medium-Low, Medium-High, and High. While the SME’s “Low” score represents the best possible result, the SME continuously works to ensure it maintains privacy protections consistent with applicable legislation and prevailing best practice, as informed Ontario’s Office of the Information and Privacy Commissioner.

7. Based on the conclusions of the TPA Assessment Report, the SME has determined that it is appropriate to expand access, on a cost recovery basis, to de-identified SME data to Canadian Status Non-Governmental Entities. A requestor will qualify as a Canadian Status Non-Governmental Entity if the requesting entity, and where relevant, the ultimate controlling parent entity of the requestor, has attested (through an authorized representative of each of the relevant parties) to having their main office or headquarters located in Canada.

8. The SME will also provide TPA to de-identified SME data to other entities beyond Canadian Governmental Entities and Canadian Status Non-Governmental Entities, when such access is required to support government or OEB directed initiatives and activities. For example, if the SME is directed by the OEB or government to share SME data with an LDC or gas distributor working group, and an entity in the group is ultimately controlled by an entity that does not have its main office or headquarters located in Ontario.

9. The SME will continue to provide TPA to the IESO, OEB and Canadian Governmental Entities, in accordance with the framework detailed in the EB-2021-0292 proceeding.

Stikeman Elliott

Stikeman Elliott LLP
Barristers & Solicitors
5300 Commerce Court West
199 Bay Street
Toronto, ON Canada M5L 1B9

Main: 416 869 5500
Fax: 416 947 0866
www.stikeman.com

Patrick G. Duffy
Direct: +1 416 869 5257
PDuffy@stikeman.com

December 16, 2024

By Email and RESS

File No.: 1019261078

Ontario Energy Board
2300 Yonge Street, 27th Floor
Toronto, ON M4P 1E4

Attention: Nancy Marconi, Registrar

Dear Ms. Marconi:

Re: Independent Electricity System Operator, in its Capacity as the Smart Metering Entity ("SME")
Application to provide access to de-identified electricity consumption data to third parties that are Canadian Governmental Entities
OEB File No. EB-2021-0292

In its Decision and Order dated March 24, 2022, the Board approved a Settlement Proposal in which the SME agreed to undertake an assessment of the Third Party Access ("**TPA**") program with the benefit of two full years of experience with the program and to report on its findings by no later than April 30, 2025.

On behalf of the SME, we enclose a copy of a report dated December 13, 2024 that satisfies this commitment. For the reasons detailed in the report, the SME may seek Board approval to expand the TPA program beyond the currently approved parties in a future application to the Board.

Yours truly,

Patrick G. Duffy

PGD/sb

Enclosure
cc. All Intervenors to EB-2021-0292

Smart Metering Entity (SME)

Assessment of Expanding Third Party Access to SME Data Beyond Currently Approved Parties

EB-2021-0292

ieso
Connecting Today.
Powering Tomorrow.

Table of Contents

1. Introduction

On March 24, 2022, the Ontario Energy Board (the "OEB") issued its Decision and Order ("Decision") in the EB-2021-0292 proceeding granting the Smart Metering Entity (the "SME") approval to expand third party access ("TPA") to de-identified smart meter data beyond the OEB and the Independent Electricity System Operator (the "IESO"), to Canadian Governmental Entities ("CGEs") [1].

The Decision approved a Settlement Proposal in which the SME agreed to undertake an assessment of the TPA program with the benefit of the SME's experience in providing access to CGEs and to report on its findings by no later than April 30, 2025, as part of its 2024 Annual Cost and Variance Account Report. The SME agreed to include in its report, at a minimum:

- an assessment of expanding TPA to other non-commercial entities[2] and, in the event the SME is not proposing to expand access, an explanation of its rationale for not doing so; and
- an assessment of implementing an option for customers to opt out of providing TPA to their data held by the SME, including seeking input from local distribution companies ("LDCs") on the feasibility of implementing this option.

The Decision indicated the OEB's preference that the SME file the results of its assessment earlier than the established deadline.

This letter report ("Report") presents the results of the SME's assessment of expanding TPA beyond currently approved parties. As further described in this Report, the SME has concluded:

1. There is strong market interest in SME data and expanding TPA will provide benefits to both SME ratepayers and energy sector participants.
2. Expanding TPA to SME data is unlikely to create any incremental risks to consumers, local LDCs, the SME or the IESO.
3. Based on the input received from LDCs, it is not practical to implement a TPA opt-out option for customers.

On the basis of its findings, the SME may seek OEB approval to expand TPA beyond currently approved parties through a future application. Such an application would be consistent with the objects of the

[1] The Decision defines CGE's as: "Federal and provincial governments, including ministries, agencies, boards, commissions, tribunals and wholly-owned corporations, or in the case of non-share capital corporations, where such corporations are controlled by a federal or provincial governments, as well as municipalities (or regional governments), universities, school boards, hospitals and First Nations. First Nations means a "council of the band" as that term is defined in subsection 2(1) of the Indian Act (Canada). "Canadian Governmental Entities" does not include private sector entities, publicly traded companies, individual doctors, professors, or government officials and all those entities that do not fall in one of the categories outlined above."

[2] The SME agreed to assess expanding TPA to SME data to, at a minimum, other "non-commercial entities". The SME expanded this minimum requirement to include a variety of non-governmental entities, to ensure a comprehensive assessment was completed.

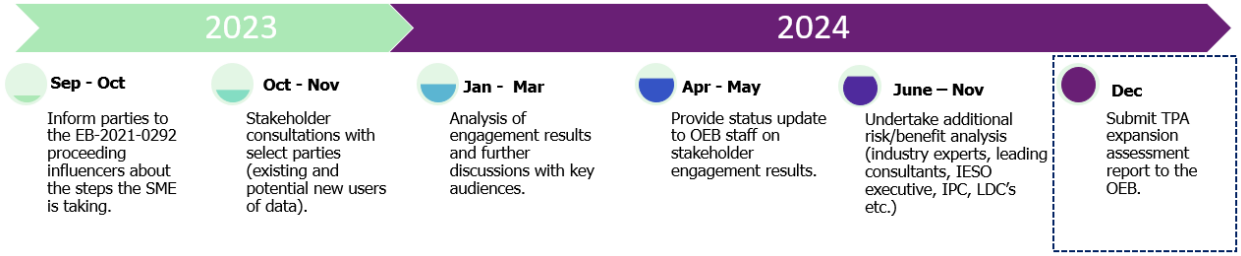
SME as outlined in the *Electricity Act, 1998*, which include, among other things, to provide and promote non-discriminatory access by distributors, retailers, the IESO and other persons to SME data.

2. Scope of Assessment and Related Findings

This Report focuses on the results of the SME's assessment of expanding TPA beyond currently approved parties. Information on the existing TPA program, the SME data available through it and how the SME ensures data privacy and security is available here: SME TPA Program.

Figure 1 illustrates the components of the multifaceted assessment undertaken by the SME over the past 18 months to evaluate the benefits and potential risks of expanding TPA access to SME data. As applicable, these components are further described in Sections 2.1 and 2.2, respectively.

Figure 1: Components of the Multi-Faceted Assessment



2.1 Benefits of Expanding Third Party Access (TPA)

The SME completed its benefits assessment by 1.) identifying the opportunities provided by expanded access, and 2.) considering the potential value of these opportunities to the energy sector and SME ratepayers. The benefits assessment was facilitated through two distinct processes:

1. Stakeholder Consultations
2. Expert Consultant Assessment

2.1.1 Stakeholder Consultations

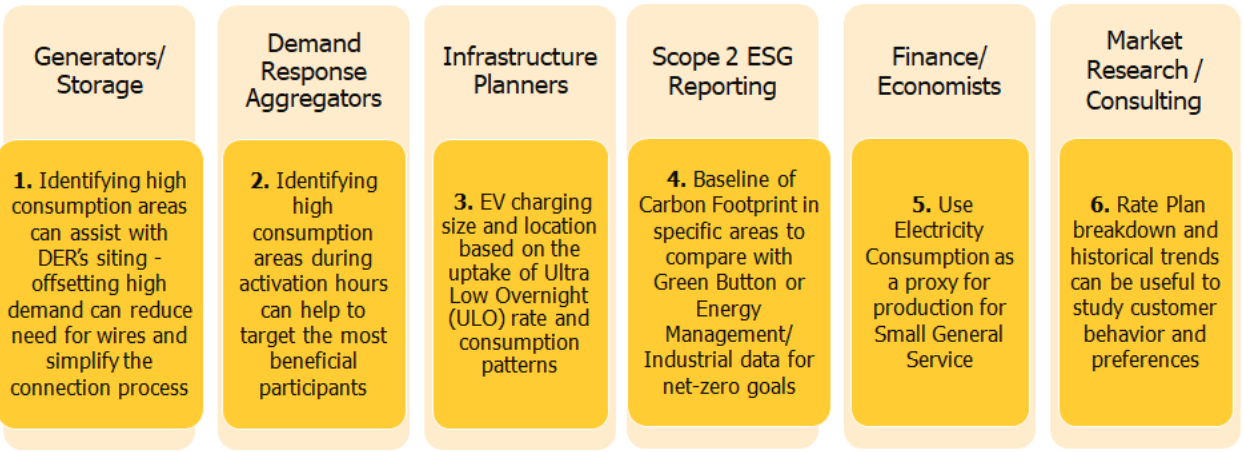
In October and November 2023, the SME conducted four stakeholder engagement sessions with a cross-section of industry stakeholders, including, but not limited to, utilities, consultants and sector participants (e.g., distributed energy resource/demand response/battery storage companies and generators).[3] During these sessions, the SME collected feedback from participants on the perceived value of gaining access to the SME data. Key observations from these sessions follow:

- A total of 112 attendees from 87 unique organizations attended.
- 93% of responding attendees indicated that they were either very interested or somewhat interested in gaining access to SME data.

[3] The SME consulted with OEB staff and certain intervenors to the EB-2021-0292 proceeding before launching the engagement sessions.

- To facilitate discussion, the SME presented and tested the efficacy of the data use cases shown in Figure 2 with participants. All use cases received positive response, with use cases 2, 3 and 1 receiving the highest interest, respectively.

Figure 2: Use Cases Tested



- Participants also volunteered additional use cases where SME data could prove beneficial, including, but not limited to, developing accurate Ontario demand models, forecasting load, leveraging smart meter data for population modeling, informing microgrid planning and resilience strategies, and utilizing SME data to support the design and evaluation of energy efficiency initiatives.

Session participants were highly engaged, provided constructive suggestions and, overall, indicated a high level of interest in gaining access to SME data.

Further information on the SME's engagement efforts are available here: IESO Third Party Access Stakeholder Engagement.

2.1.2 Expert Consultant Assessment

The SME engaged Accenture to conduct an assessment of the opportunities of expanding TPA to SME data.

Accenture responded to the following questions through a combination of primary and secondary research that included, as examples, interviews, the consideration of market trends, observations from the SME's stakeholder consultation sessions, and current SME data use cases:

1. Can expanding TPA to SME data spur new business opportunities within Ontario?
2. Can expanding TPA to SME data spur competition in the energy market?
3. Can expanding TPA to SME data help the IESO maintain business relevance within the Ontario market and beyond as a leader?

Following its research, Accenture organized the identified opportunities under the below listed seven key themes. The key themes are ordered based on their likelihood of occurrence and potential value they provide to SME ratepayers.

1. Energy efficiency & conservation
2. Operational & infrastructure management
3. Innovation & technological advancement
4. Compliance & regulatory
5. Stakeholder engagement & satisfaction
6. Market dynamics & competition
7. Financial & economic

Accenture concluded its assessment by stating "[d]ata-driven findings from SME consumption data can unlock new energy efficiency programs, spur new competition and business across the province, and ultimately serve the best interests of Ontarians as it relates to their energy usage and insights that can be developed from an aggregated load forecasting level".

2.2 Third Party Access (TPA) Expansion Risk Assessment

The SME engaged Accenture and Privacy Analytics Inc. independently to identify and analyze any risks to data privacy and electric grid security associated with expanding TPA to SME data, including risks associated with use of artificial intelligence (AI).

Combined, the studies concluded that expanding TPA to SME data is not expected to create incremental risk to customers, LDCs or the IESO.

2.2.1 Accenture

Accenture undertook a comprehensive assessment of the risks of expanded TPA to SME data from three perspectives: grid security, market manipulation and de-anonymization. The assessment leveraged, among other resources, global power and utilities industry specialists, AI and generative AI advisors, and research teams.

Accenture's investigations resulted in a finding that from all three perspectives incremental risk was "unlikely" to occur, and concluded its assessment by stating "…expanding TPA to SME data beyond Canadian Governmental Entities does not appear to result in any scenarios that would likely increase the existing overall risk profile of the IESO or SME. Rather, it appears that the expansion of TPA to SME data would yield many positive opportunities in the market that may benefit Ontario ratepayers."

2.2.2 Privacy Analytics Inc. (PA)

PA's analysis focused on assessing the effectiveness of the SME's current data security and privacy protections in defending SME data against growing AI threats.[4] Based on its assessment, PA assigned the SME an "AI Risk Determination" score of "Low", stating "given the de-identification methods employed by the IESO SME to manage risks from sharing aggregated data, the risk from AI systems in using this data is low". The de-identification methods utilized by the SME, and upon which PA's conclusion was based, are described here: SME TPA Program.

Four tiers of AI Risk Determination exist; Low, Medium-Low, Medium-High, and High. While the SME's Low score represents the best possible result, the SME continuously works to ensure it maintains privacy protections consistent with prevailing best practice.

2.3 Market Interest in SME Data

Access to SME data by CGEs was officially launched on October 13, 2022. To date, market interest in SME data has been strong even with the narrow eligibility requirements and limited offer visibility (TPA is only advertised on the IESO's website).

The SME's Annual Cost and Variance Account Report for 2023 detailed the 17 TPA requests it had received from 15 different entities since launch. Since the filing of the 2023 Report in May 2024, the SME has received an additional nine TPA requests from six different entities, illustrating the continued strong market interest for SME data.[5]

[4] PA's analysis was informed by the OECD.AI Framework for the Classification of AI Systems and NIST AI Risk Management Framework

[5] The additional nine requests were made by municipalities, LDCs, an electricity generator and universities/university students.

3. Feasibility of TPA Opt-Out

The SME addressed the feasibility of an TPA opt-out option through consultations with both the Meter Data and Management Repository (MDM/R) Technical Panel and the MDMD/R Steering Committee (SSC). Technical Panel[6] and SSC[7] membership is exclusive to LDCs.

LDCs provided the following feedback on the opt-out option during consultations:

- Medium and larger LDCs could facilitate opt-outs through an electronic customer election process (i.e., without human interaction) through modifications to their Customer Information Systems (CIS).
    - These LDCs have categorized the opt-out modification as a "mid-size change/non-emergency" and could take 24-months or longer to implement.

- Some smaller LDCs indicated that no simple implementation option exists, due to limitations with their current CISs.
    - These LDCs would prefer/require a manual process to implement the opt-out option.

- The OEB would be required to approve implementation cost recovery mechanisms.

- LDCs expressed concerns over potential customer confusion with existing opt-outs for other LDC programs currently in market.

- Customer communications would be required for managing any opt-out option. implications.

For the above reasons, LDCs expressed a strong preference that a TPA opt-out option not be implemented.

Based on the input received from LDCs, the SME has concluded that it is not practical to implement a TPA opt-out option for customers.

[6] MDM/R Technical Panel members at the time of consultation: Toronto Hydro, Elexicon Energy, Halton Hills Hydro, Alectra Utilities, Hydro One, Hydro Ottawa, Fortis Ontario, Milton Hydro, Waterloo North Hydro, Energy Plus.

[7] SSC members at the time of consultation: Synergy North, Alectra Utilities, Hydro One, Hydro Ottawa, Elexicon, Burlington Hydro, London Hydro, Orangeville Hydro, Toronto Hydro.

Independent Electricity System Operator
1600-120 Adelaide Street West
Toronto, Ontario M5H 1T1

Phone: 905.403.6900
Toll-free: 1.888.448.7777
E-mail: customer.relations@ieso.ca

ieso.ca

@IESO_Tweets
linkedin.com/company/IESO

ieso
Connecting Today.
Powering Tomorrow.

ACCENTURE: ASSESSMENT OF RISKS & OPPORTUNITIES WITH EXPANDING THIRD PARTY ACCESS TO SMART METERING ENTITY DATA

1. Accenture's report entitled *Assessment of Risks & Opportunities with Expanding Third Party Access to Smart Metering Entity Data* dated September 23, 2024 provides an independent assessment of the IESO's planned privacy strategy for TPA. This report was commissioned to support the SME's evaluation of expanding TPA as directed by OEB under EB-2021-0292.

2. As per the TPA Assessment Report, the Accenture report includes a detailed analysis of:

   (a) Opportunities associated with expanding TPA to SME data; and

   (b) Risks related to data privacy, electric grid security, and potential market manipulation, including risks associated with artificial intelligence.

3. The full version of the Accenture report is being filed on a confidential basis in accordance with the OEB's *Practice Direction on Confidential Filings*.

AI Threats and Risk Implications

AI Risk Tiering for Anonymized Electricity Consumption Data

2024-03-08

PRIVACY ANALYTICS
an IQVIA company

AI Risk Determination

This *AI Risk Determination* refers to the risk that an AI system may cause harm to people or the environment based on the introduction of de-identified or aggregated IESO Smart Metering Entity (SME) data. An AI system may be used in ways that risk causing harm to people or the environment without the use of IESO SME data. The focus of this report, however, is to consider the elevated risk if IESO SME data is introduced to an AI system. The purpose of the risk tiering done in this report is to prioritize and manage risks effectively.

Given the de-identification methods employed by the IESO SME to manage risks from sharing aggregated data, we determine that the risk from AI systems in using this data is low. This is primarily due to the reduced privacy concerns and the reduced potential impact in revealing detailed information, and the generalized nature of aggregated data results in less specific and precise outputs (minimizing the potential for bias and discrimination). Ensuring purposes for using the data are defined is nonetheless recommended, which the IESO SME already does, as part of its current control protocols on all use-cases for smart metering data sharing.

Should the IESO SME decide to share row-level data, we determine that greater consideration be given to appropriate uses and, in particular, that additional governance be required of AI systems based on their risk profile. Row-level data is by its very nature more granular and informative. It is also more likely to be combined with other sources of information in training an AI system. While we believe the risks from AI systems to be manageable, ranging for medium to high in the risk tiering exercise of this report, an AI governance framework would ensure that risks and impact are properly considered.

The preliminary risk rating in the AI risk tiering of this report is determined early in the evaluation process and helps to categorize an AI system into an appropriate risk tier. This preliminary rating guides subsequent, more detailed evaluations and determines the extent and intensity of validation and monitoring efforts required for the AI system. It serves as a foundational step in managing and mitigating AI risks effectively, ensuring that resources are allocated efficiently and AI systems with higher risks receive more attention.

Limitations

Our determination of risk to the de-identified and aggregated IESO SME data from AI systems is based on reasonableness of the foreseeable circumstances at the present time in which IESO SME shares this data. To the best of our knowledge, we have applied generally accepted principles and practices for evaluating AI risks, which are documented in this report along with the assumptions made. The risk tiering provides a preliminary rating before mitigation and control measures, with a direction on a suitable AI governance framework. AI risk and impact assessments were out of scope for this engagement and would be more suitable if applied directly to an AI system. As a risk management approach, residual AI risk will always be present.

Executive Summary

PRIVACY ANALYTICS
an IQVIA company

Issue summary and solution outline

AI Threat

Why the concern

- **AI** is the application of computational tools to address tasks traditionally requiring human analysis. Given the breadth of interpretation, from regression to large language models, the size and impact of an AI system can vary a great deal.
- **Regulators** have taken note of the uncertainty with neural network models in general, and generative AI models in particular. The proposed EU AI Act and Canada AI & Data Act are clear examples and inform our analysis.
- **Data**, including anonymized, can be misused. AI can heighten this given the lack of explainability or transparency, and ease of use, bringing greater risk to people.

Managing Threat

What can be done

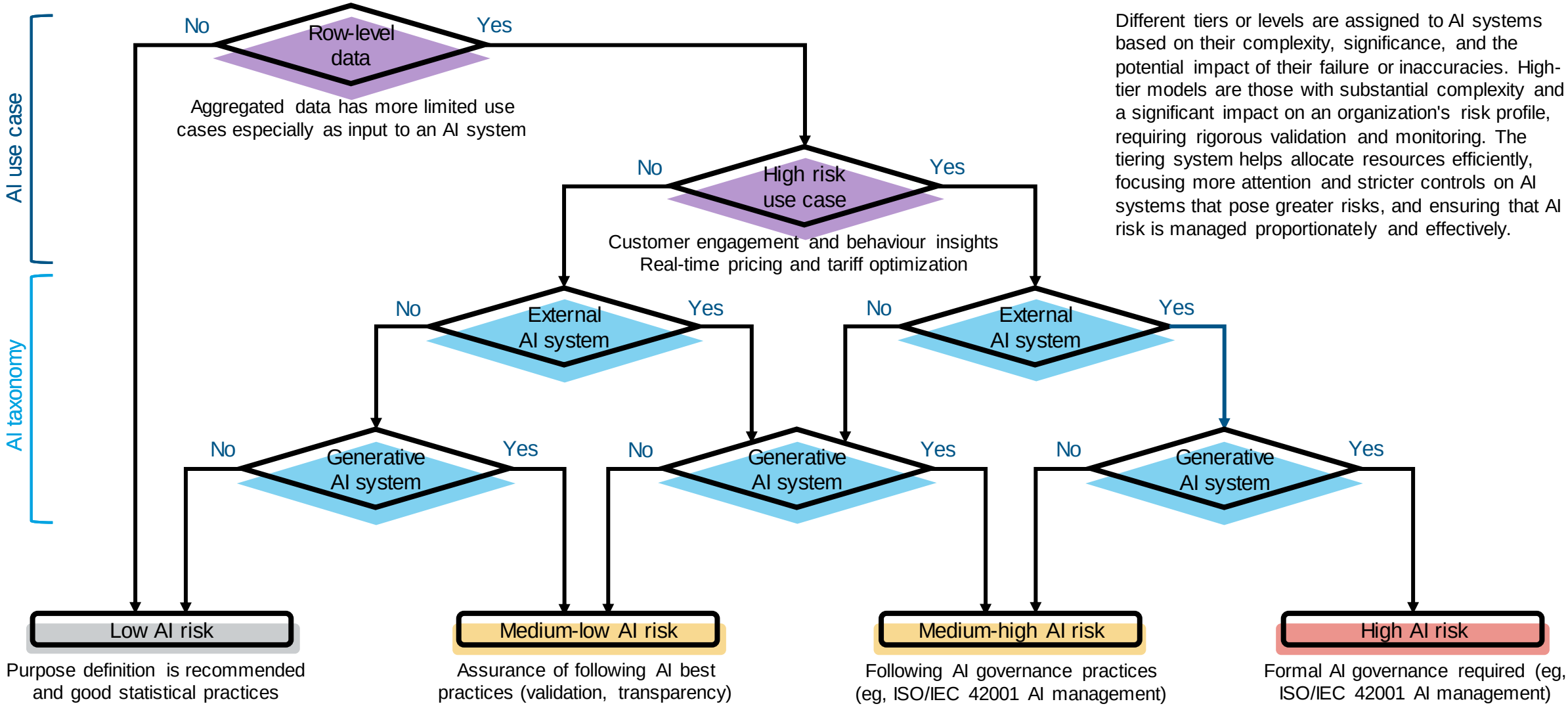
- **Misuse** of data can take many forms, and a policy lens can be applied to identify risk factors by classifying AI systems in terms of how badly they can go wrong. The use case for the AI system plays a critical role in determining risk.
- **Attacks** on an AI system will depend on the access to it (internal vs external system) and the AI technology. Given regulatory concerns and NIST taxonomy, predictive AI vs generative AI is good way to divide the attack surface.
- **Tiering** AI risk can follow best practice from financial services, a highly regulated field with extensive experience delivering on model risk management.

Data Sharing

How to mitigate

- **Contractual** obligations can specify purpose definitions for using the anonymized (aggregate or row-level) data as well as AI governance that is required, through formal certifications, attestations, or outlining necessary best practices.
- **Inform and train** data users on the risks of AI and their obligations in terms of best practices. This is an acknowledged method to reduce AI risks and recommended practice by regulators (in some cases, it may become a legislated requirement).
- **Verify** that practices are being adhered to for higher risk use cases and AI systems, by requiring proof of certification, assessment, or documented practices.

AI risk tiering: preliminary rating before mitigation and control measures (enforced governance)



Different tiers or levels are assigned to AI systems based on their complexity, significance, and the potential impact of their failure or inaccuracies. High-tier models are those with substantial complexity and a significant impact on an organization's risk profile, requiring rigorous validation and monitoring. The tiering system helps allocate resources efficiently, focusing more attention and stricter controls on AI systems that pose greater risks, and ensuring that AI risk is managed proportionately and effectively.

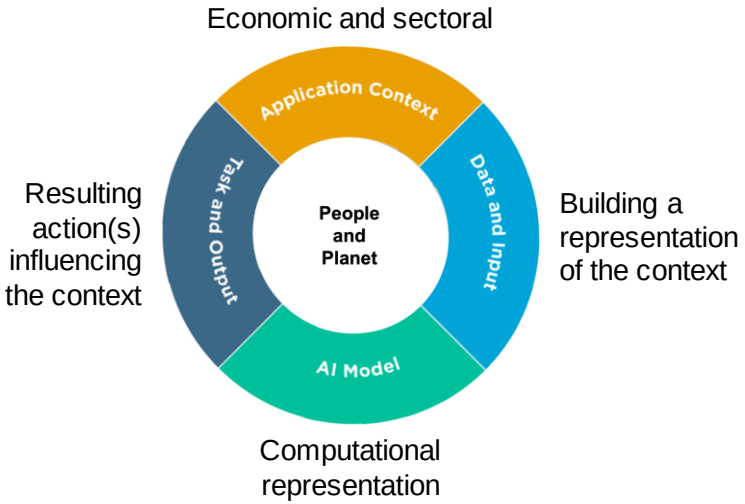
PRIVACY ANALYTICS
an IQVIA company

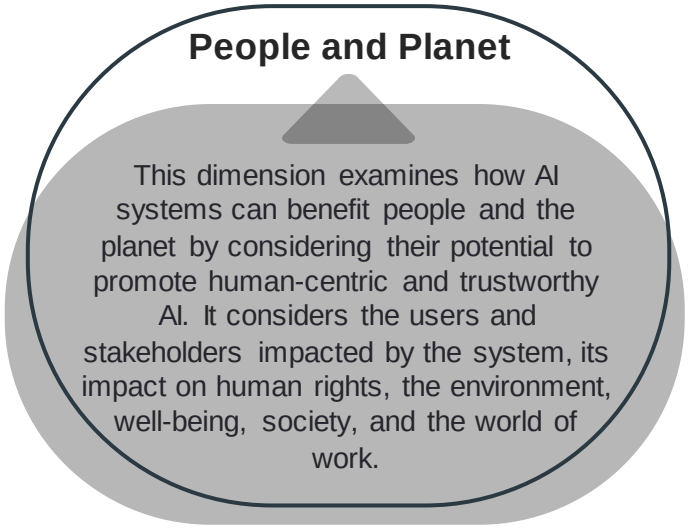
ISO/IEC 42001 AI management system is a standard to use, develop, monitor or provide products or services that utilize AI. The standard requires the use of AI risk assessments, treatments, and impact assessments. https://www.iso.org/obp/ui/en/#iso:std:iso-iec:42001:ed-1:v1:en

Framework for classification of AI system risk

PRIVACY ANALYTICS
an IQVIA company

5 dimensions for the classification of AI systems and how these and a lifecycle view were applied





AI system classification

The OECD Framework for the Classification of AI Systems is a policy-oriented tool for evaluating AI systems along five dimensions: People & Planet, Economic Context, Data & Input, AI Model, and Task & Output. This framework helps policymakers, regulators, and legislators understand the multiple impacts of AI systems. It links AI characteristics to the OECD AI Principles, focusing on values such as human rights, fairness, transparency, and safety. The framework promotes a nuanced understanding of the role of AI in different sectors, and helps shape tailored AI policies and regulations.

How we used it

We applied the framework dimensions and criteria to outline possible risks from using AI with anonymized electricity consumption data. We excluded real-time smart metering from consideration, which limits the relevant pool of academic research regarding use cases and risks.

AI system risk assessment

The NIST AI Risk Management Framework (AI RMF) is a comprehensive guide to managing the risks associated with AI systems. It is designed to help organizations across sectors navigate the complexities of AI adoption and ensure responsible and ethical use. The AI RMF enhances the OECD guidance by delineating specific stages for AI system development and deployment, including Planning and Design, Data Collection and Processing, Model Building and Usage, Verification and Validation, Deployment and Usage, and Operations and Monitoring. This makes it a valuable tool for organizations seeking to align their AI practices with broader goals of societal well-being and responsible innovation.

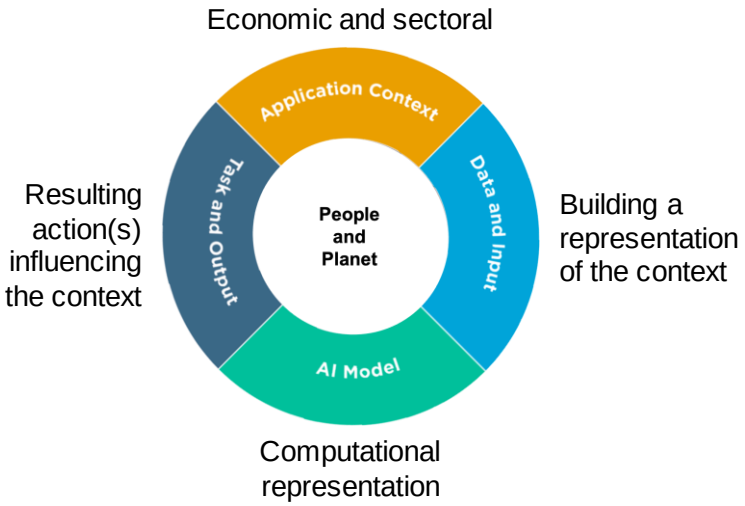
How we used it

We considered the comprehensive nature of the NIST AI RMF and focused on core elements needed to tier AI risk based on relevant data sharing. The NIST Adversarial Machine Learning taxonomy of attacks was also informative. Given that the The NIST AI RMF is a framework, we recommend the consideration of ISO/IEC 42001 AI management system with explicit requirements for managing high risk AI applications.

PRIVACY ANALYTICS
an IQVIA company

OECD. Framework for the Classification of AI Systems. Organisation for Economic Development. Available at: https://oecd.ai/en/classification

5 dimensions for the classification of AI systems and a summary of the criteria used



Economic Context

This dimension focuses on the economic and sectoral environment in which an applied AI system is implemented. It is specific to an applied AI application and describes the type of organization and functional area for which an AI system is developed. The report considers factors such as the sector in which the system is deployed, its business function and model, criticality, deployment, impact and scale, and technological maturity.

Data and Input

This dimension explains the important factors that an AI model considers while building a representation of the environment. It includes the origin of data and inputs, how they were collected (either by machine or human), their structure and format, and data properties. These characteristics can be divided into two categories- data used for training the AI model and data used in production.

People and Planet

This dimension examines how AI systems can benefit people and the planet by considering their potential to promote human-centric and trustworthy AI. It considers the users and stakeholders impacted by the system, its impact on human rights, the environment, well-being, society, and the world of work.

Task and Output

This dimension refers to the parts of a system, including the tasks it performs, its outputs, and resulting actions that impact the overall context. The characteristics of this dimension include system tasks, action autonomy, and core application areas such as computer vision. Evaluation methods are also important in this dimension. Examples of systems that combine tasks and actions include autonomous vehicles.

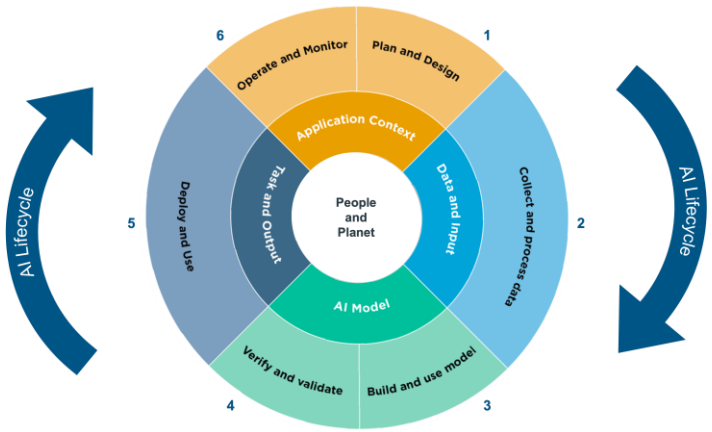
AI Model

This dimension describes the concept of an "environment model" in AI systems, which is a computational representation of the external environment that the AI system interacts with. This model can include various elements such as processes, objects, people, and interactions. Core characteristics include understanding the technical type of the model, how it is built, and how it is used.

PRIVACY ANALYTICS
an IQVIA company

OECD. Framework for the Classification of AI Systems—Classification Framework Dimensions and Criteria at a Glance. Organisation for Economic Development. 2022, Feb. Available at: https://wp.oecd.ai/app/uploads/2022/02/Classification-2-pager-1.pdf

NIST AI Risk Management Framework extends the OECD Classification of AI Systems for detailed assessments



Economic Context

Plan and Design: This stage involves articulating and documenting the system's concept and objectives, underlying assumptions, and context in light of legal and regulatory requirements and ethical considerations.

Operate and Monitor: This stage is dedicated to overseeing the system's performance and assessing its recommendations and impacts, both anticipated and unforeseen.

Data and Input

Collect and Process Data: This stage involves gathering, validating, and cleaning data while meticulously documenting its metadata and characteristics.

Align these processes with the specific objectives of the AI system. Legal and ethical considerations play a role, ensuring compliance and ethical integrity in how data is acquired and processed.

People and Planet

The assessment examines how AI systems can benefit people and the planet by considering their potential to promote human-centric and trustworthy AI. It considers the users and stakeholders impacted by the system, its impact on human rights, the environment, well-being, society, and the world of work.

Task and Output

Deploy and Use: This stage involves piloting the AI system, ensuring compatibility with existing legacy systems, and verifying adherence to regulatory requirements.

This involves managing organizational changes from AI integration and critically evaluating the user experience. It ensures that the deployment of AI systems is smooth, compliant, and beneficial to the intended users.

AI Model

Build and Use Model: This stage involves the creation or selection of algorithms and the training of models.

Verify and Validate: This stage is where the model's outputs are verified and validated. This includes calibrating the model and interpreting its outputs to ensure they are accurate and reliable. These steps are important for maintaining integrity and effectiveness.

NIST. AI Risk Management Framework. National Institute of Standards and Technology, NIST AI 100-1. 2023, Jan. Available at: https://www.nist.gov/itl/ai-risk-management-framework

Use cases and classification

Use cases identified for anonymized electricity consumption data

Academic literature review

- As an electricity system operator who manages and shares anonymized grid data with public bodies and private enterprises, there are several key use cases for this data, drawn from the various sources and studies you've referred to:
- Energy Demand Prediction: AI and machine learning can be used to accurately forecast energy usage, optimizing energy distribution and consumption at different scales, from local to national levels.
- Smart Grid Enhancement: Enhancing smart grid platforms, integrating renewable energy sources effectively. This includes managing domains like generation, transmission, distribution, and consumption.
- Market Design and Value Utilization: Improving trust in digital platforms and reducing matchmaking friction in the energy market, enhancing user experience and efficiency.
- Operational Efficiency: AI facilitates optimized grid operation and management, enhances energy supply prediction, load balancing, and market pricing for the electricity market.
- Energy Reductions and Carbon Emission Reductions: Influence consumer behavior to achieve energy usage reductions, which leads to less energy production, reduced carbon emissions, and improved air quality.
- Demand-Side Flexibility and Smart Grids: Implementing intra-day pricing and automated load control to enable flexibility in the domestic energy sector. This helps in managing demand and integrating intermittent renewables.
- Network Management and Monitoring: Improving the management of electricity distribution infrastructure, including fault identification, restoration of electricity supply, and informed investment decisions.
- Energy Research and Public-Interest Uses: Expanding energy research and exploring new information. Smart meter data can be crucial in assessing the impact of policy interventions and reforms in the energy sector.
- Predictive Maintenance: Anticipating maintenance needs and potential equipment failures in the distribution network, thereby reducing operational costs and improving reliability.
- Non-Technical Losses Detection: Identifying and addressing electricity theft or losses not due to technical issues, crucial for the financial health of power companies.
- Flexibility Management and Planning: Managing the flexibility market, including aggregating flexible loads and Distributed Energy Resources (DERs) for better grid stability and efficiency.
- Energy Management Systems (EMS): Enhancing building energy efficiency and demand response programs, using AI for automatic decision-making in scheduling and controlling energy assets.
- Aggregated Flexibility Services: Offering flexibility services to energy agents like residential and industrial consumers, BRPs, and DSOs by aggregating flexibility from different customers.
- Trading and P2P Energy Exchange: Developing methods for energy exchange between different stakeholders, focusing on decentralized energy trading like peer-to-peer (P2P) transactions.
- Asset and Investment Planning: Examining grid status and expansion criteria for optimal planning, including the selection of appropriate technologies and geographical locations for new infrastructure.
- Supporting Public Bodies and Private Enterprises: Providing valuable data for various stakeholders to develop new services, optimize existing operations, and create innovative business models in the energy sector.

These uses cases were primarily taken from academic publications on the uses of electricity consumption data. We narrowed the selection of academic publications by excluding papers around smart meters and the electricity grid, which focused primarily on real-time activity.

More use cases for anonymized electricity consumption data

Industry literature review

- Local Energy Planning: Community-wide utility data can be instrumental in targeting local planning efforts for energy saving and maximizing energy efficiency efforts. This data can help track, map, and compare energy usage by sector or geographic area, providing baseline measurements for community-based energy efficiency efforts.
- Targeting and Evaluating Energy Efficiency Initiatives: Aggregated data can be used by local governments and utilities to identify energy efficiency opportunities across building portfolios and communities. This data can be layered with other demographic or building data to target energy efficiency programs towards underserved customers, including high energy users.
- Driving New Energy Models and Customer Service Innovations: Regulators use data access to drive new energy models that rely on customer service innovations. Improved data access can support various initiatives like advanced metering infrastructure (AMI) and smart grid developments.
- Benchmarking for Building Owners: Utilities provide benchmarking tools to building owners, allowing them to collect energy usage data automatically. This helps in comparing electricity usage between properties, outlining energy usage trends, and evaluating the impact of energy efficiency upgrades.
- Energy-Use Tracking for Single-Family Homes: Tools like MyHomeEQ provided by utilities help single-family homeowners track their home energy usage, compare it with community aggregates, and receive tailored energy efficiency recommendations.
- Real Estate Market Innovation: In some regions, home energy reports are generated for listed properties, similar to vehicle information on car window stickers, providing prospective buyers with information about a home's energy use.
- Multi-Tenant Building-Level Energy Management: Aggregate-level data can enable energy management at a larger scale, such as in multi-tenant buildings, without compromising individual privacy. This data is crucial for understanding and managing energy usage patterns in such buildings.
- Supporting Various Stakeholders: The data can be used by different stakeholders, including state agencies, local governments, research institutions, solar installers, and building owners, for various purposes like planning, benchmarking, and implementing energy efficiency measures.

These additional use cases, as outlined by ACEEE (American Council for an Energy-Efficient Economy) and other energy authorities, highlight the broad range of applications for anonymized electricity consumption data in improving energy efficiency, supporting local and community planning, aiding in real estate transactions, and driving innovations in energy services.

PRIVACY ANALYTICS
an IQVIA company

See the Reference section for a list of papers used to identify use cases

Classifying the use cases for using anonymized electricity consumption data by risk tier for people, planet, system operator

Risk tiering of use cases

Risk to People

- Fraud detection and theft prevention: **low to medium risk** since primarily beneficial for consumers although could impact customer relations.
- Smart home automation (including energy management systems): **medium risk** due to potential privacy breaches and handling of detailed consumption data that could reveal personal habits.
- Customer engagement and behavioural insights (including market design and value utilization or demand-side flexibility): **medium to high risk** from attribution or if personal data is not adequately anonymized.

Risk to Planet

- Environmental impact assessment: **low risk** because it supports sustainability.
- Integration of renewable energy sources: **low risk** as it promotes environmental health.
- Urban planning and energy policy development: **low risk** because it aids in sustainable development.
- Relevant use cases are beneficial for the planet, aiding in sustainability and environmental health, or have a neutral or indirect impact on the environment.

Risk to Operator

- Demand response programs: **medium risk** due to operational complexity, the need for precise and reliable data handling, and the direct impact on consumers.
- Load forecasting and planning: **medium risk** because of the potential for operational inefficiencies and long-term planning impacts from inaccurate load forecasting.
- Real-time pricing and tariff optimization (including trading and P2P energy exchange or market design and value utilization): **high risk** due to the implications from financial and operational complexities.

This is an application of the OECD Framework for the Classification of AI Systems based on the identified use cases.

High Risk to People: customer engagement and behaviour insights

Trading and peer-to-peer (P2P) energy exchange

- Privacy risk: Even when anonymized, data in these use cases could potentially be re-identified, especially if combined with other datasets.
- Market impact: Improper use or leaks of this data could manipulate market prices or unfairly advantage certain players.
- Social equity: Could lead to unequal access or benefits within energy markets, disproportionately affecting vulnerable populations.

Energy management systems (EMS) and demand-side flexibility

- Invasion of privacy: Detailed consumption data might reveal personal habits or occupancy patterns.
- Control over personal choices: There's a risk of perceived or actual overreach into personal choices and home autonomy.

Market design and value utilization

- Operational challenges: Mismanagement or leaks of data could lead to operational inefficiencies and economic losses.
- Reputation concerns: Mishandling data could lead to loss of public trust and legal repercussions.

Non-technical losses detection

- Operational and financial risk: Incorrect identification of losses or theft could lead to false accusations or customer dissatisfaction.
- Data security and compliance: Breaches in data security could lead to significant operational and legal challenges.

Network management and monitoring

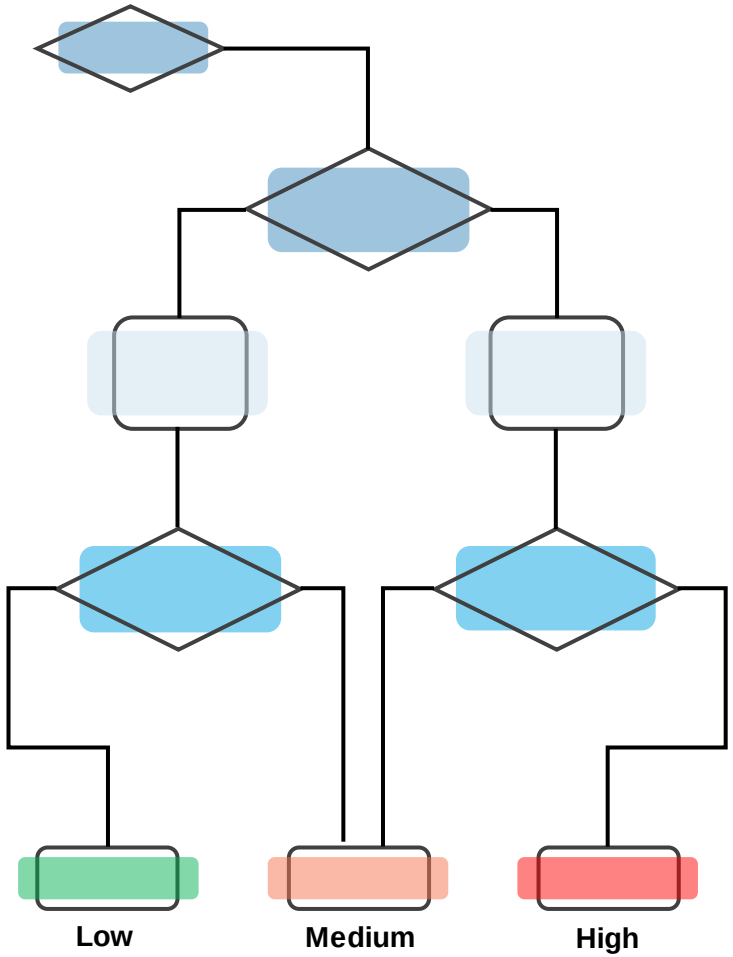
- Infrastructure reliability: Misinterpretation of data could lead to incorrect decisions in network management, potentially causing outages or system failures.
- Strategic planning accuracy: Inaccurate data analysis can lead to suboptimal investment decisions and resource allocation in long-term planning.

High Risk to System Operator: real-time pricing and tariff optimization

AI risk tiering

PRIVACY ANALYTICS
an IQVIA company

The application of model risk management from finance is being extended into AI model risk management



In finance

Model risk tiering is part of risk management in financial services. It involves categorizing financial models based on the risk they pose, enabling better resource allocation and risk management. Key insights from industry practices include:

- Models are assigned to various risk tiers, not ranked individually.
- Tiering tools, like scorecards or decision trees, consider both the risk and impact of model failure.
- Calibration of these tools is largely judgmental.
- Governance over model risk tiering tools is evolving with rising standards.

In practice, this tiering system aids in risk-sensitive model management by varying validation activities based on a model's risk level. It ensures that models posing higher risks receive more attention, while simpler models with lower risk levels undergo less rigorous validation. This approach helps in efficient allocation of resources and mitigates the risks associated with financial modeling.

More broadly

Objective data and expert judgment play important roles in risk tiering. This approach is especially relevant for AI models due to their complex and often unpredictable nature. Miscommunications between model owners and AI model risk management teams, regarding model profile elements, can lead to changes in risk-tier assignments. Rapid technological advancements and diverse applications can significantly alter risk profiles for AI models. The risk tiering of these models may also assess risks relative to other models that are inventoried, emphasizing the context-dependent nature of risk in AI applications.

Risk tiering can be treated as a model in itself, subjected to validation and review. This can increase transparency and create alignment across a function or organization. For AI models handling personal data, this includes potential data privacy breaches or incorrect personal data processing.

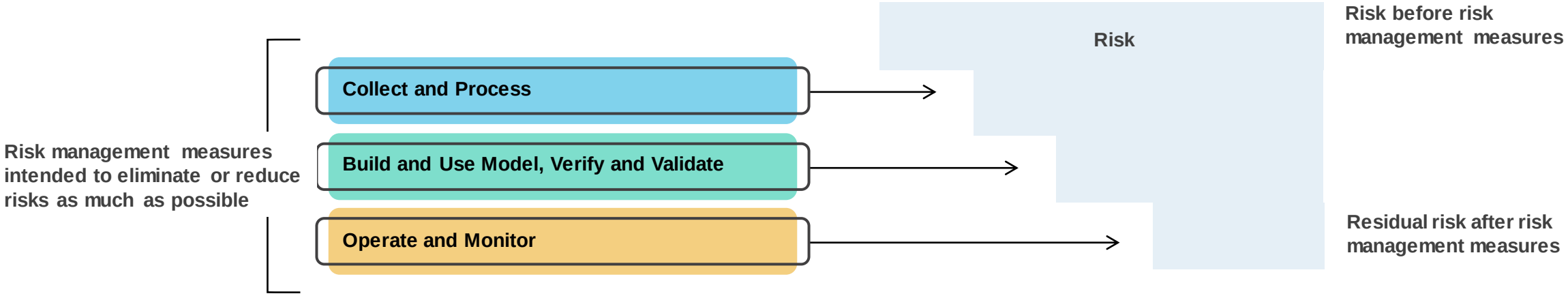
Note how AI models might receive multiple risk-tier assignments based on their various uses, affecting the depth and frequency of validation activities. The distribution of models across risk tiers requires a balanced view otherwise it can be overwhelming and results in resistance to adoption. Consistency and predictability in tier assignments becomes important the more rules and decisions are in place, so that model owners and developers can align their activities with relevant risk management expectations. Industry experience suggests a simple approach is most effective, with additional scrutiny for higher risk AI systems.

Kiritz N, Ravitz M, Levonian M. Model Risk Tiering: An Exploration of Industry Practices and Principles. Journal of Risk Model Validation. 2019 Jun 6. Sateli B, Del Castillo F, Moshtagi R. Towards Determining the Criticality of AI Applications: A Model Risk Management Perspective. The 36th Canadian Conference on Artificial Intelligence. 2023 June 5-9.

Regulatory perspectives on AI risk can be mapped to proposed legislation and risk management measures

Regulatory

Proposed legislation, in EU and Canada, are emphasizing a risk-based approach to AI systems classification. Focus is placed on ensuring safety, transparency, traceability, non-discrimination, and environmental sustainability. High-risk systems will undergo thorough assessment throughout their lifecycle, including periodic risk assessments, implementing control measures, and post-market monitoring, with an emphasis on user-centric considerations. This regulatory approach marks a significant shift towards more comprehensive and stringent AI governance, with global implications for AI development and use.

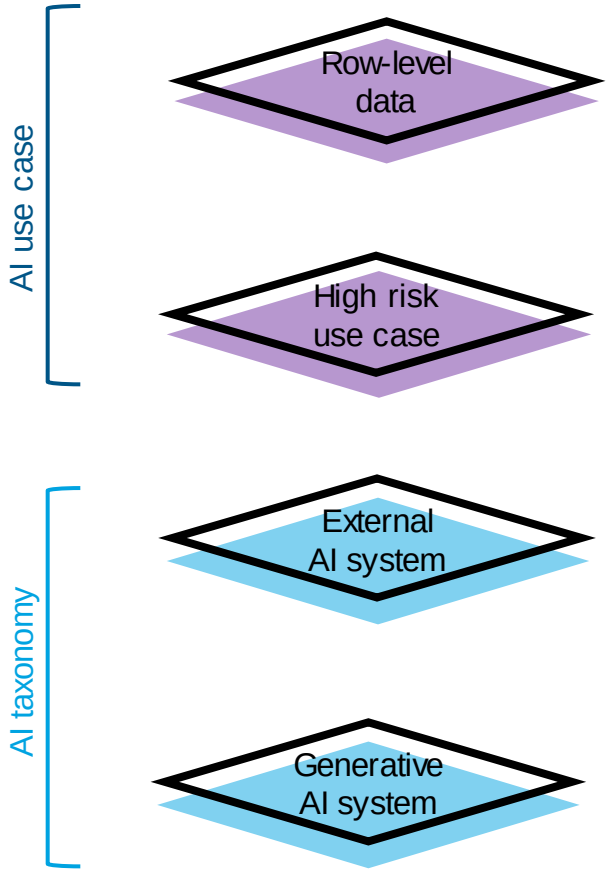


Risk management

The regulatory framing maps to the OECD AI system classification, which was developed for policy analysis and used in developing the proposed risk-based legislation, and therefore the NIST AI Risk Management Framework. We can map the key steps of the NIST AI RMF along the AI lifecycle and see how these decrease AI system risk. We have used this framing and the expectations that it sets to make recommendations in the AI model risk tiering decision tree, namely in terms of the recommended policies to apply data sharing based on the AI risk tier.

Niet I, van Est R, Veraart F. Governing AI in Electricity Systems: Reflections on the EU Artificial Intelligence Bill. Frontiers in Artificial Intelligence. 2021 Jul 30;4:690237.
Schuett J. Risk Management in the Artificial Intelligence Act. European Journal of Risk Regulation. 2023 Feb:1-9.

Decision nodes in constructing an AI risk tiering decision tree incorporating use cases and threats



The decision tree is structured to allow for a systematic evaluation of various aspects of an AI system, including its usage and possible threats, to determine the appropriate risk tier.

AI use case

Using a binary variable at the topmost decision point can create a strong binary effect. Aggregated data (or *macrodata*) is, however, generally considered less risky for use in AI systems compared to row-level data (or *microdata*), leading to its classification in a lower risk tier. This is primarily due to the reduced privacy concerns and the reduced potential impact in revealing detailed information, and the generalized nature of aggregated data results in less specific and precise outputs (minimizing the potential for bias and discrimination).

Row-level data, on the other hand, is by its very nature more granular and informative. It is also more likely to be combined with other sources of information in training an AI system. High-risk use cases are therefore singled out in a binary decision point to ensure those that will adversely impact people, the planet, or the system operator are evaluated more closely in the risk tiering process.

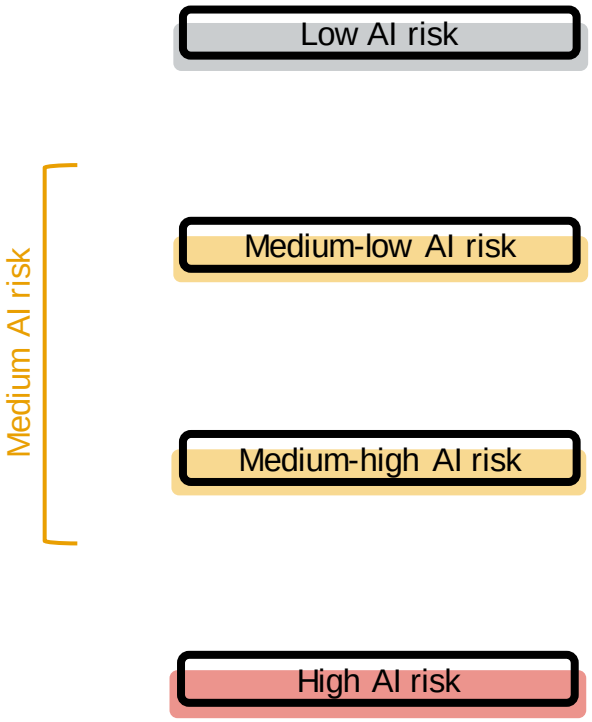
AI taxonomy

A web-based AI system exposed to external threats inherently faces greater risks due to its accessibility over the internet, making it more susceptible to unauthorized access, where malicious actors could potentially manipulate, steal, or corrupt the data, compromising both the integrity and confidentiality of the system. It is also at risk of exposure to malicious inputs or adversarial attacks, which can deliberately mislead the AI algorithms, leading to incorrect or biased outputs. Similarly, these systems are more prone to exploitation for unethical uses or privacy violations.

Predictive AI and generative AI are susceptible to different types of attacks and require unique mitigation strategies. This division allows for a more nuanced and effective analysis of adversarial threats and the development of tailored countermeasures for each AI category, eg, abuse violations are specific to generative AI. Generative AI is of particular concern to regulators due to recent advancements and demonstrated capabilities.

Vassilev A, Oprea A, Fordyce A, Andersen H. Adversarial Machine Learning: A Taxonomy and Terminology of Attacks and Mitigations. National Insttute of Standards and Technoloigy, AI 100-2 E2023. 2024, Jan. Available at: https://csrc.nist.gov/pubs/ai/100/2/e2023/final

Conclusion nodes in constructing an AI risk tiering decision tree for preliminary risks before mitigation and control measures



Risk tiers

The preliminary risk rating in the AI risk tiering is determined early in the evaluation process and helps to categorize an AI system into an appropriate risk tier. This preliminary rating guides subsequent, more detailed evaluations and determines the extent and intensity of validation and monitoring efforts required for the AI system. It serves as a foundational step in managing and mitigating AI risks effectively, ensuring that resources are allocated efficiently and Ai systems with higher risks receive more attention.

An AI management system can be required to use, develop, monitor or provide products or services that utilize AI. This would enforce the use of AI risk assessments, treatments, and impact assessments. We have therefore organized the AI risk tiering with recommendations on different assurance levels, including formal certification to international standard ISO/IEC 42001 in the case of high risk AI systems. Where certification to a standard is deemed unnecessary, a readiness assessment may be sufficient or contractual obligations on following a set of recommended practices.

Purpose definition is recommended throughout the tiers, even though high risk use cases were singled out. Defining the purpose of an AI system involves clearly outlining what the system is intended to do, its target application, and the expected outcomes. This clarity aids in identifying potential risks associated with the system's operation, including ethical considerations, biases, and misuse scenarios. Understanding the system's purpose allows for more targeted risk assessments, ensuring that the identified risks are relevant and the mitigation strategies are effective.

Jurisdictions

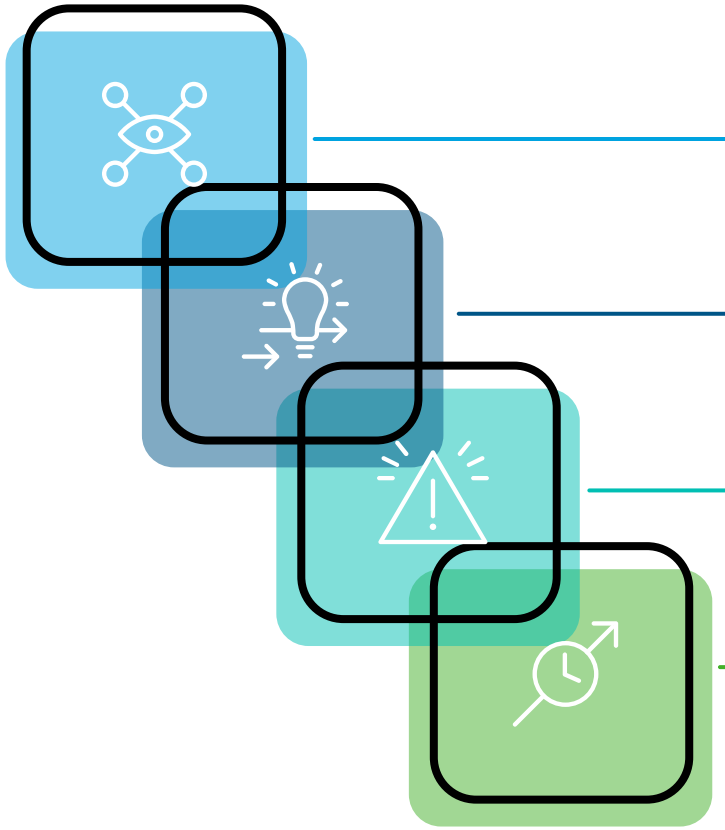
Enforceable agreements when sharing data for an AI system across jurisdictions ensure legal compliance with each privacy standards, intellectual property rights, and data usage regulations. They provide a clear framework for data handling, storage, processing, and transfer, reducing legal risks and misunderstandings. Enforceable agreements also safeguard against data misuse, ensure ethical data handling practices, and maintain data security, which are crucial for maintaining trust and integrity in AI systems operating internationally.

Where agreements cannot be enforced, the risk tier can be increased. It should be clear to the recipient that lack of adherence to agreements will result in no further data sharing. Readiness assessments and certification to international standards can also mitigate risks where these have been adopted in the target jurisdictions, since these are completed by independent experts.

FTC. AI Companies: Uphold Your Privacy and Confidentiality Commitments. Federal Trade Commission, Technology Blog. 2024, Jan 4. Available at: https://www.ftc.gov/policy/advocacy-research/tech-at-ftc/2024/01/ai-companies-uphold-your-privacy-confidentiality-commitments

Ensure norms for the safe and responsible use of anonymized data are respected and maintained

While it is always possible that something may go wrong, anonymization is a risk management exercise with practices adopted from cybersecurity. This has been recognized in best practice guidance, including the international standard ISO/IEC 27559 data de-identification framework, which includes governance practices. Although we have helped clients with readiness assessments and with crisis management assistance, the circumstances of each situation can vary greatly. When there is a leak of information, a risk assessment is conducted to determine the extent of the leak and whether it warrants a breach response. Similarly, if the circumstances of data use have significantly changed, a risk assessment on the data environment, access, and sharing will determine whether there is a need to evaluate the data for potential disclosures. Evaluating multiple steps before concluding that the data itself is at risk due to contextual changes is important. These cases are often complex, and a quick response is necessary to contain and control the situation before making final determinations. However, these incidents can be managed and are typically rare with anonymization that is tailored to the risk profile of the data environment.



MONITOR DATA ENVIRONMENT

Anonymization considers who will have access to the data, under what circumstances, and what other data could be available to them. Monitor these considerations to ensure the identifiability assessment remains valid or whether any changes are needed.

HORIZON SCAN

Changes in regulations, legal precedents, technology, and data can change the evaluation of identifiability as well as expectations for anonymization. Scan the horizon for any new developments that will affect your assessments of anonymization or use and sharing of anonymized data to update practices accordingly.

MITIGATE INCIDENT

In the event of a potential disclosure, immediate action can contain the incident and minimize damage by following previously defined plans. It's important to determine the extent of the incident and whether it constitutes a breach, taking into account the context and the data involved.

CONTINUOUSLY IMPROVE

Periodically review and make updates as needed. This can be done through regular assessments of data, either on a 12-24 month interval or by using a platform or bulk approach to confirm the data environment remains safe for its intended uses.

PRIVACY ANALYTICS
an IQVIA company

Borel S, Arbuckle L. Good Governance for Anonymized Data: Ensuring Data is Safe Before and After Anonymization. Privacy Analytics White Paper. 2023, May 4. Available at: https://privacy-analytics.com/resources/white-papers/good-governance-for-anonymized-data/

Other references

List of sources used to identify use cases

- Niet I, van Est R, Veraart F. Governing AI in Electricity Systems: Reflections on the EU Artificial Intelligence Bill. Frontiers in Artificial Intelligence. 2021 Jul 30;4:690237.
- Teng F, Chhachhi SA, Ge PU, Graham J, Gunduz D. Balancing Privacy and Access to Smart Meter Data: Nn Energy Futures Lab Briefing Paper. 2022 May 26.
- Xu Y, Ahokangas P, Louis JN, Pongrácz E. Electricity Market Empowered by Artificial Intelligence: A Platform Approach. Energies. 2019 Oct 30;12(21):4128.
- McKenna E, Richardson I, Thomson M. Smart Meter Data: Balancing Consumer Privacy Concerns with Legitimate Applications. Energy Policy. 2012 Feb 1;41:807-14.
- Alahakoon D, Yu X. Smart Electricity Meter Data Intelligence for Future Energy Systems: A survey. IEEE Transactions on Industrial Informatics. 2015 Mar 18;12(1):425-36.
- Barja-Martinez S, Aragüés-Peñalba M, Munné-Collado Í, Lloret-Gallego P, Bullich-Massague E, Villafafila-Robles R. Artificial Intelligence Techniques for Enabling Big Data Services in Distribution Networks: A Review. Renewable and Sustainable Energy Reviews. 2021 Oct 1;150:111459.
- Corti L, Bishop L. Elam S. Legal and Ethical Challenges Surrounding Big Data: Energy Data. UK Data Service, Data Service as a Platform Case Study. 2017 Nov. Available at: https://ukdataservice.ac.uk/case-study/legal-and-ethical-challenges-surrounding-big-data-energy-data/
- American Council for an Energy-Efficient Economy. Facilitating Access to Community Energy Usage Data. ACEE Toolkit. 2015 Jan 1. Available at: https://www.aceee.org/toolkit/2015/01/facilitating-access-community-energy-usage-data
- American Council for an Energy-Efficient Economy. Energy Usage Data Access: A Getting-Started Guide for Regulators. ACEE Toolkit. 2017 Feb 16. Available at: https://www.aceee.org/toolkit/2017/02/energy-usage-data-access-getting-started-guide-regulators
- American Council for an Energy-Efficient Economy. Improving Access to Energy Usage Data. ACEE Toolkit. 2020 Feb 5. Available at: https://www.aceee.org/toolkit/2020/02/improving-access-energy-usage-data

Questions? Please contact

Luk Arbuckle, Chief Methodologist

Email: larbuckle@privacy-analytics.com
LinkedIn: http://linkedin.com/in/lukarbuckle/

PRIVACY ANALYTICS
an IQVIA company

COST RECOVERY MODEL FOR THIRD PARTY ACCESS

1. The SME currently provides access to data sets that are made public on its website at no charge with associated costs recovered through the approved Smart Metering Charge (the "**SMC**"). These products include de-identified, pre-aggregated smart meter data in standard formats such as CSV or XLSX.

2. For customized data requests that require staff time and resources to prepare (which can involve visualizations such heat maps, trend analysis, etc.), the SME charges the cost recovery fee of $145/hour as approved in EB-2021-0292 with the exception of requests made by the IESO or the OEB, which are fulfilled at no charge in accordance with the OEB's direction.

3. The SME proposes to extend the cost recovery fee of $145/hour to TPA requests from Canadian Status Non-Governmental Entities and other entities when such access is required to support government or OEB directed initiatives and activities.

4. The SME's cost recovery approach will ensure that incremental burden is borne by the requestor, thereby minimizing the impact on ratepayers. The $145/hour rate reflects the internal staff time and resources required to fulfill the TPA requests and is designed to avoid cross-subsidization by ratepayers of the SMC.

5. Prior to executing a DUA, the requester will receive a detailed cost estimate which includes a clause to enforce payment of any fees, disbursements and other charges invoiced by the IESO.

6. Any revenue collected from the TPA activities is being tracked in the SME's Operating Reserve Balancing Account ("**ORBA**") and considered for future disposition as part of the ORBA in accordance with the OEB's Decision and Order in EB-2022-0137.

TERMS OF ACCESS PRINCIPLES

1. The terms of access for TPA will remain unchanged from those detailed in the SME's evidence in EB-2021-0292 and which the OEB, in approving the settlement proposal in that proceeding, determined were appropriate. The SME will provide TPA to the SME data on appropriate terms, through:

   (c) a principled assessment of each data access request, based on privacy, security, ethical use, compliance, ratepayer value, accessibility, and data quality;

   (d) continued engagement of the Ethics Committee in instances where additional scrutiny on the appropriateness of a TPA request is required; and

   (e) the contractual terms of the DUA.

2. These principles ensure that access is granted in a manner that aligns with the SME's statutory obligations and ethical standards, which safeguard privacy and promote public and/or sector benefits.