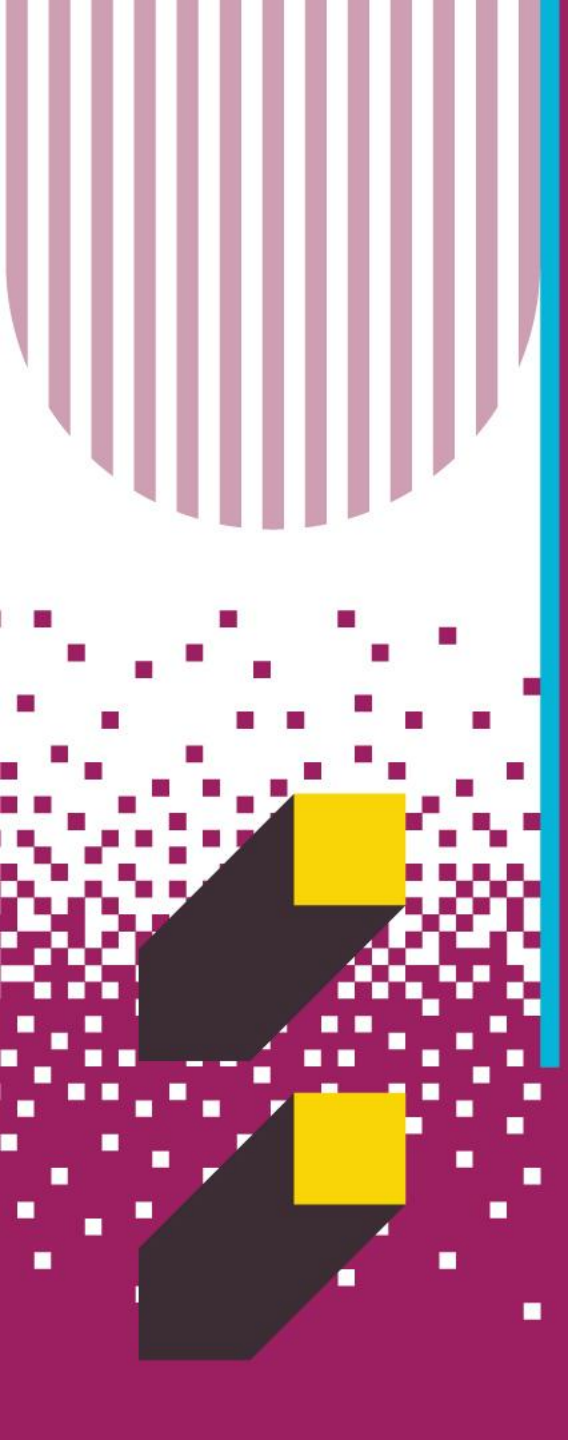


IAPP **Canada Symposium 2026**

Privacy | AI governance | Cybersecurity law

Conference 4-5 May

Workshops 6 May

Training 6-7 May

TORONTO

#IAPPSymposium26

GENERATIVE AI FOR YOUR PRIVACY OFFICE

WELCOME AND INTRODUCTIONS

Lisa Pilgram

Head of Operations, Ottawa Medical AI Research Institute

Postdoctoral Fellow, University of Ottawa

Michael Pascu

Senior Manager, Artificial Intelligence

INQ Consulting

AGENDA OUTLINE

I. Welcome and Introductions

II. Context and Motivation:
Where Privacy Teams Face Challenges and Where GenAI Can Help

III. Practical GenAI Approaches:
Structured Prompts and Retrieval-Augmented Generation

IV. Use Cases and Demonstration:
Applying GenAI To Different Types of Documents

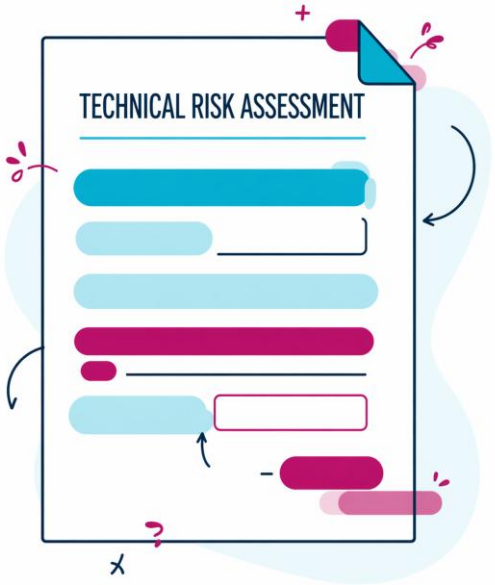
The Reality of Modern Privacy Workflows

Privacy teams are stretched in multiple directions at once - all of them demand significant **time** and **expertise**.

Understanding & Interpretation
Dense technical artifacts and inconsistent terminology that must be translated into decisions.

Review & Compliance
Documents that must be reviewed against criteria with variability in how criteria are applied across reviewers.

Understanding & Interpration



Privacy teams encounter documents that are **technically dense** and difficult to parse quickly.

Increasingly complex methods

Faster pace of change

Hidden assumptions

Specialized language

Large volume

Review & Compliance

Privacy teams review a wide range of documents that must meet **certain requirements.**

Multiple document types

Variability across reviewers

High review volume

Need for consistent decisions

Manual, checklist-driven process

Where AI Tools Can Fit

AI tools do not replace privacy expertise – but they can support **how** that expertise is applied and **accelerate** processes.

Understanding & Interpretation

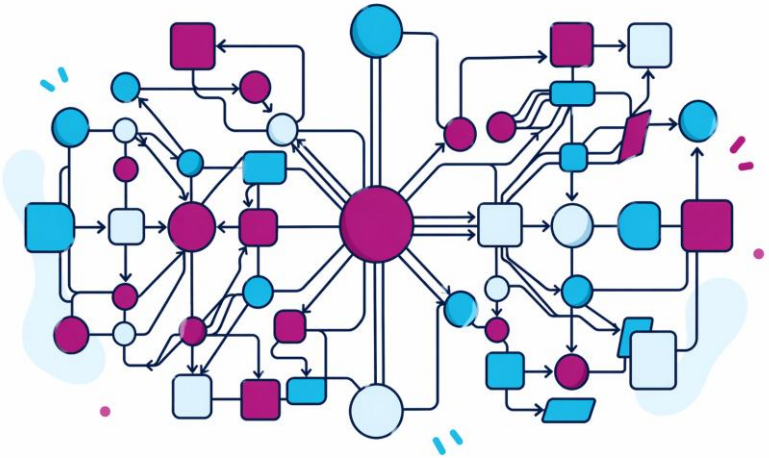
- Explain technical concepts in context
- Extract assumptions and key findings
- Support interactive Q&A over documents

Review & Compliance

- Apply pre-defined criteria consistently
- Identify missing elements or inconsistencies
- Produce structured initial assessments

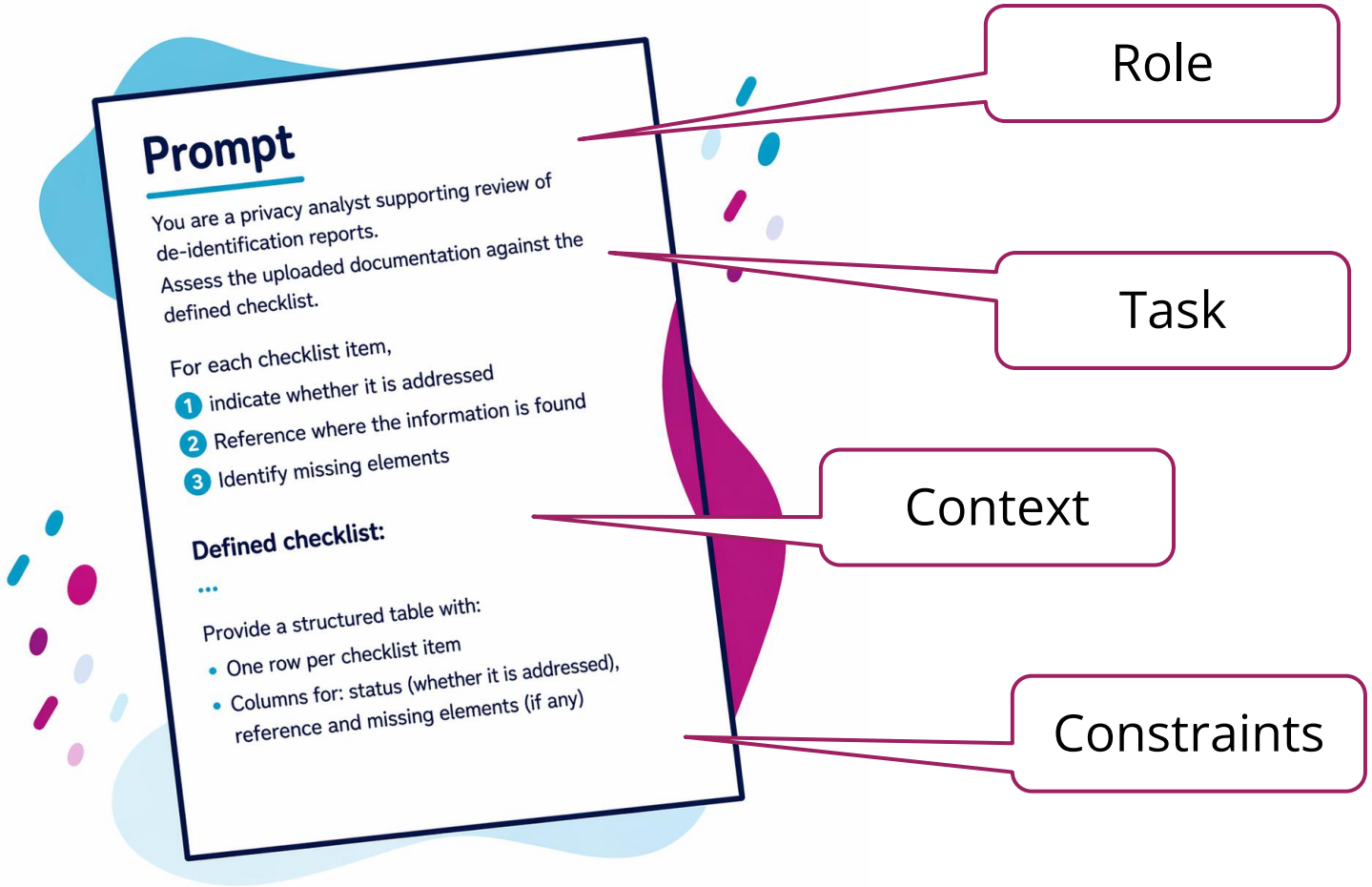
From Simple Use to More Integrated Workflows

- Structured prompts for LLMs
- Retrieval-augmented generation
- Interactive, human-in-the-loop workflows

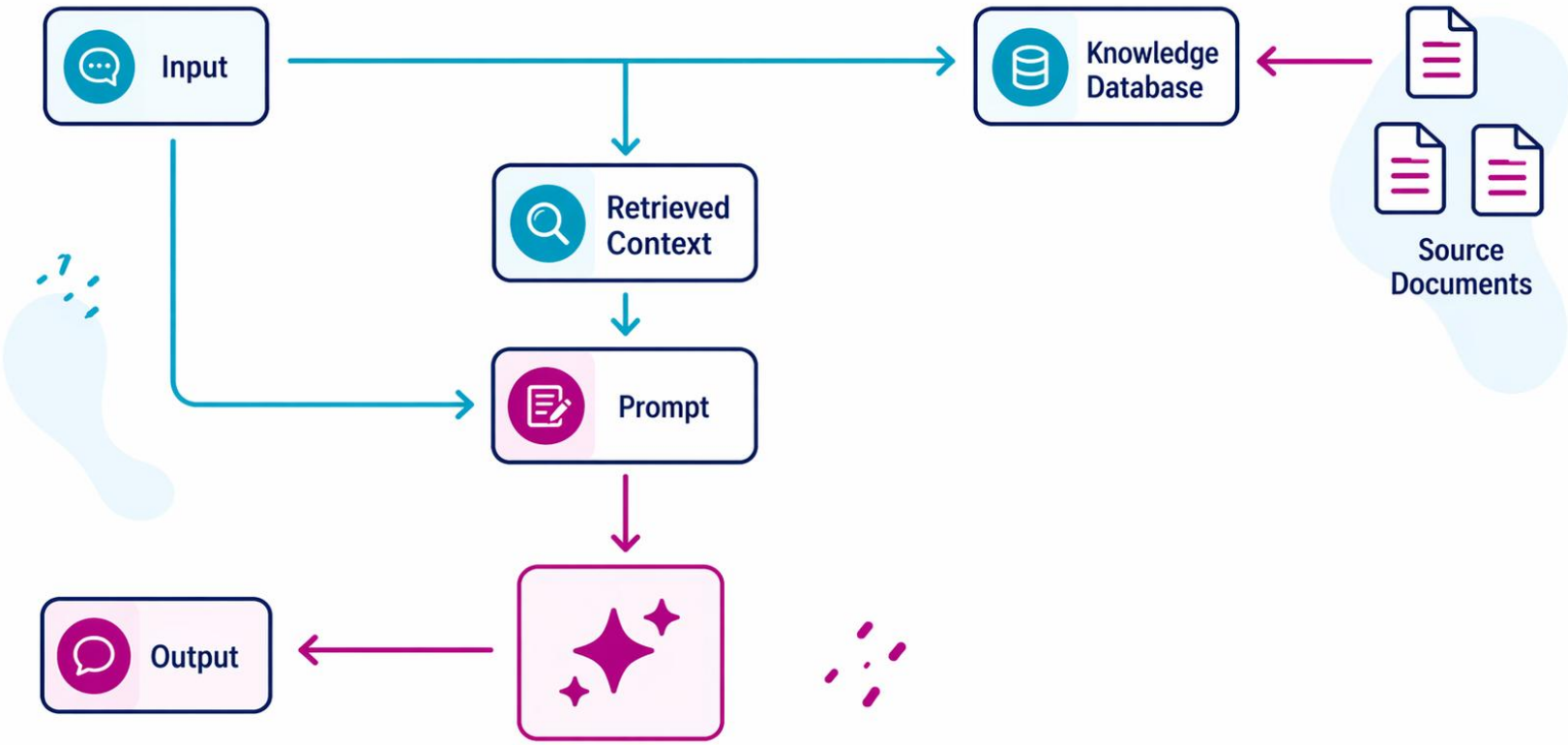


- Multi-tool workflows
- Agentic systems
- More end-to-end process automation

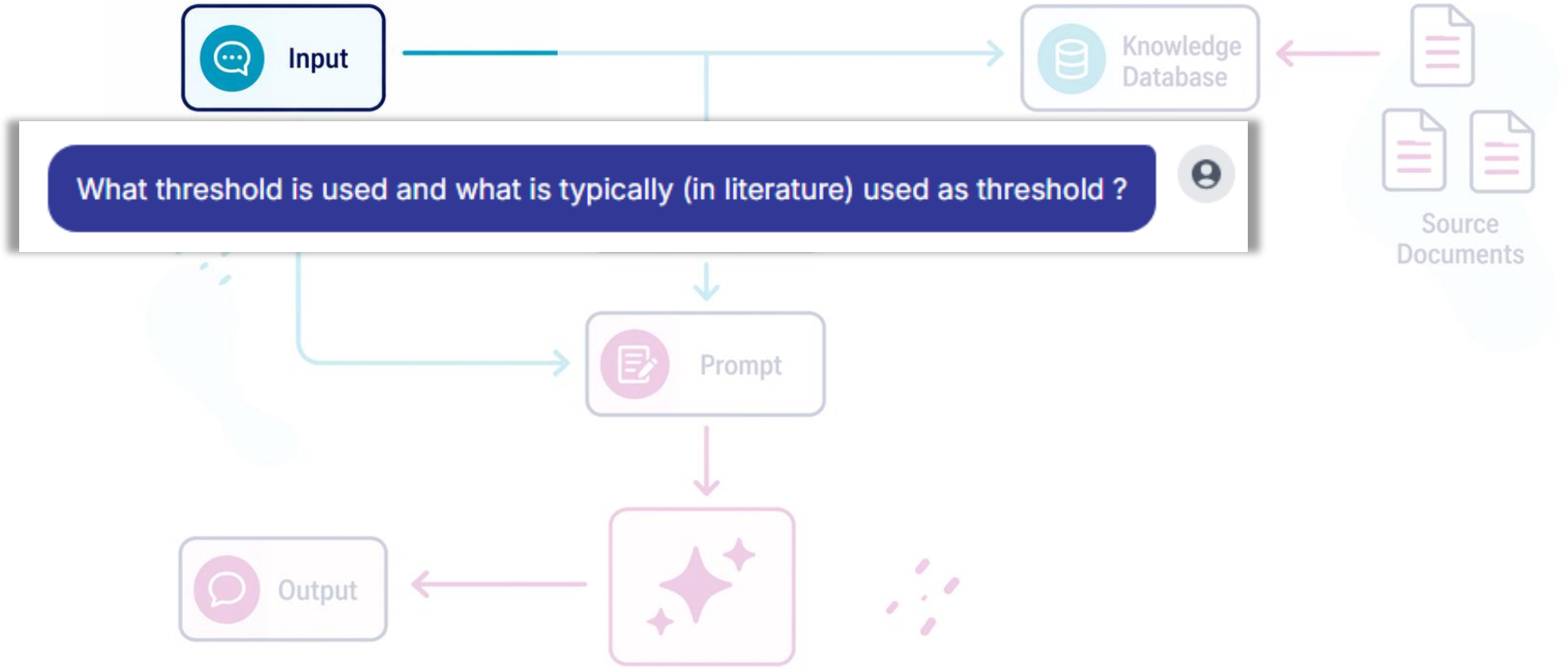
Review & Compliance: Structured Prompts



Understanding & Interpretation: Retrieval-Augmented Generation

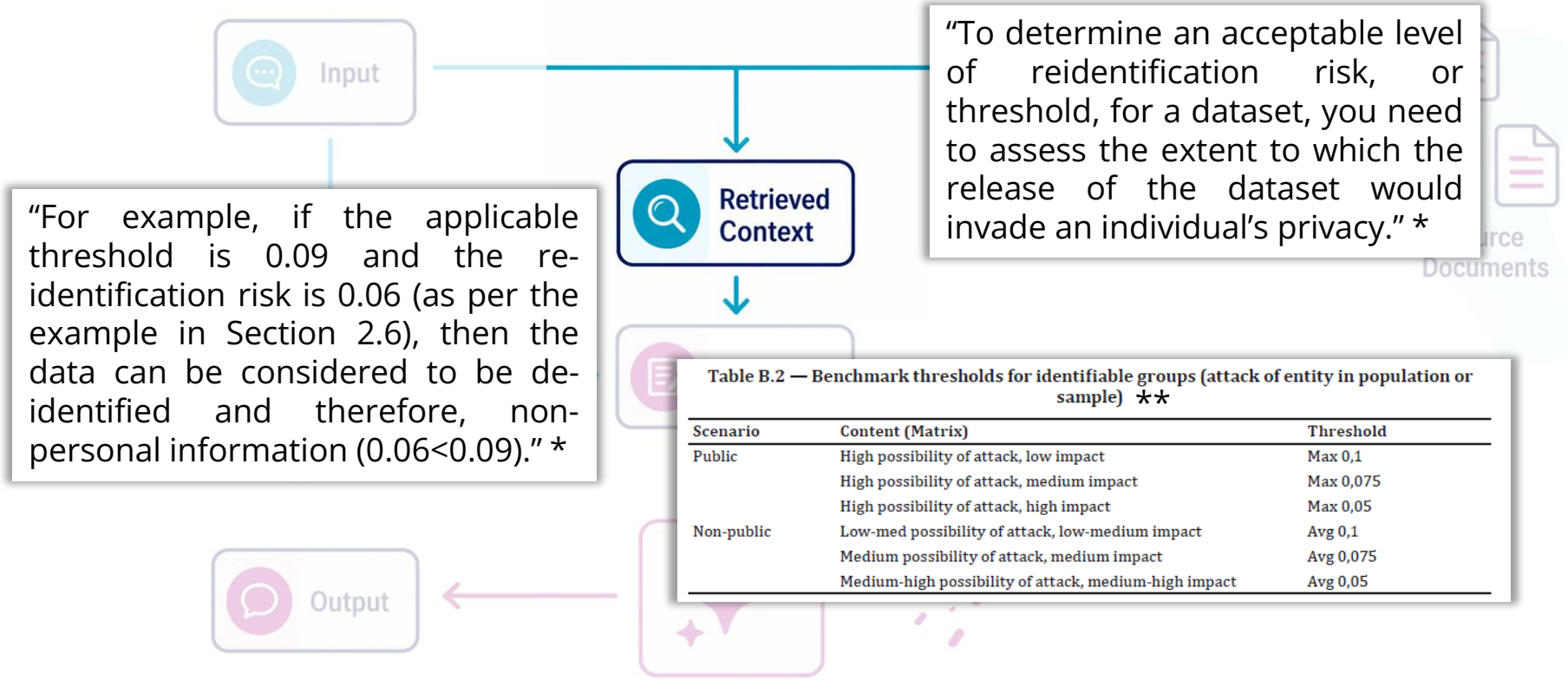


Understanding & Interpretation: Retrieval-Augmented Generation



Understanding & Interpretation: Retrieval-Augmented Generation

Understanding & Interpretation: Retrieval-Augmented Generation



"To determine an acceptable level of reidentification risk, or threshold, for a dataset, you need to assess the extent to which the release of the dataset would invade an individual's privacy." *

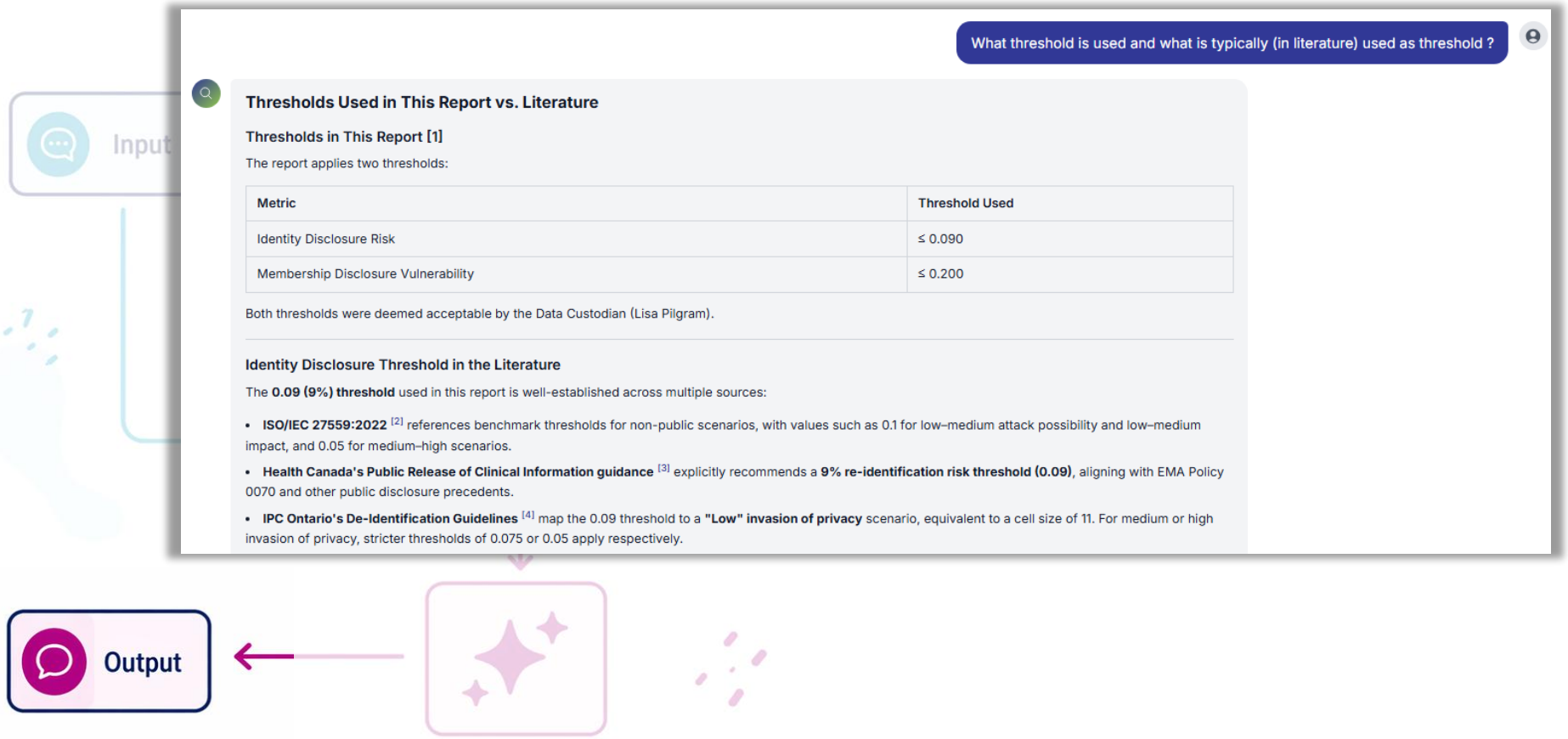
"For example, if the applicable threshold is 0.09 and the re-identification risk is 0.06 (as per the example in Section 2.6), then the data can be considered to be de-identified and therefore, non-personal information (0.06<0.09)." *

Table B.2 — Benchmark thresholds for identifiable groups (attack of entity in population or sample) **

Scenario	Content (Matrix)	Threshold
Public	High possibility of attack, low impact	Max 0,1
	High possibility of attack, medium impact	Max 0,075
	High possibility of attack, high impact	Max 0,05
Non-public	Low-med possibility of attack, low-medium impact	Avg 0,1
	Medium possibility of attack, medium impact	Avg 0,075
	Medium-high possibility of attack, medium-high impact	Avg 0,05

* from the *De-identification Guidelines for Structured Data* published by the Office of the Information and Privacy Commissioner of Ontario. 2025.
** from ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems

Understanding & Interpretation: Retrieval-Augmented Generation



Use Cases In Practice

Q&A Risk Assessment Reports
Extract information from a dense report, clarify terminology, concepts and methods and discuss interpretation and implications.
Tool: Woodway Assurance EviData®

Review De-Identification Reports
Check against defined criteria from the De-identification Guidelines for Structured Data published by the Office of the Information and Privacy Commissioner of Ontario (2025).
Tool: Open AI ChatGPT

Review De-Identification Methodology
Evaluate a de-identification methodology against defined criteria from good practice.
Tool: Open AI ChatGPT

Review Data Sharing Agreements
Check against defined criteria from the De-identification Guidelines for Structured Data published by the Office of the Information and Privacy Commissioner of Ontario (2025).
Tool: Open AI ChatGPT

Interested in Discussing Further ?

Lisa Pilgram

lpilgram@ehealthinformation.ca

Michael Pascu

mpascu@inq.consulting

How Did Things Go?
(We Really Want To Know)

Did you enjoy this session? Is there any way we could make it better? Let us know by filling out a speaker evaluation.

1. Open the IAPP Events app.
2. Select **IAPP Symposium 2026**.
3. Tap "Schedule" on the bottom navigation bar.
4. Find this session. Click "Rate this Session" within the description.
5. Once you've answered all three questions, tap "Done".

Thank you!