

ASSESSMENT 01 · CLIENT CARE OPERATIONS

AI Readiness Assessment

Seven practical dimensions to examine before introducing AI into a business workflow.

Prepared as an educational planning tool. It is not a certification, a legal opinion, or an assessment of a particular organization.

7

READINESS DIMENSIONS

0–2

SCORE PER DIMENSION

14

MAXIMUM TOTAL

How to use this assessment

- 1 Select one proposed AI use case.
- 2 For each of the seven dimensions in Section 01, mark a readiness score: 0 = not defined; 1 = partially defined; 2 = documented and evidenced.
- 3 Record the evidence and an accountable owner. Unknown answers score 0.
- 4 Total the scores and complete the decision worksheet in Section 02.

This is a planning aid, not an official NIST rating.

ASSESSMENT RECORD

PROPOSED USE CASE

PROCESS OWNER

REVIEW DATE

REVIEWER

SECTION 01

Readiness review

Mark one score for each dimension. Record the evidence that supports the score and the person accountable for closing any gap.

0 = Not defined

1 = Partially defined

2 = Evidenced (documented and evidenced)

Unknown answers score 0

1

Defined business problem

Is there a specific workflow, target user, required output and measurable business objective?

SCORE

☐ 0 — Not defined

☐ 1 — Partially defined

☐ 2 — Evidenced

ACCOUNTABLE OWNER

EVIDENCE / NOTES

2

Data quality and permission

Have authoritative sources, data quality, sensitive information, permitted uses and retention needs been considered?

SCORE

☐ 0 — Not defined

☐ 1 — Partially defined

☐ 2 — Evidenced

ACCOUNTABLE OWNER

EVIDENCE / NOTES

3

Human accountability

Is a named person responsible, with explicit approval/override rules for consequential actions?

SCORE

☐ 0 — Not defined

☐ 1 — Partially defined

☐ 2 — Evidenced

ACCOUNTABLE OWNER

EVIDENCE / NOTES

4

Evaluation criteria

Are routine, difficult and failure test cases defined with thresholds for acceptable performance?

SCORE ☐ 0 — Not defined ☐ 1 — Partially defined ☐ 2 — Evidenced

ACCOUNTABLE OWNER

EVIDENCE / NOTES

5

Security and privacy controls

Have tool access, information disclosure, output handling, logging and applicable privacy obligations been reviewed?

SCORE ☐ 0 — Not defined ☐ 1 — Partially defined ☐ 2 — Evidenced

ACCOUNTABLE OWNER

EVIDENCE / NOTES

6

Operational ownership

Are monitoring, incident response, vendor changes, fallback steps and support responsibilities defined?

SCORE ☐ 0 — Not defined ☐ 1 — Partially defined ☐ 2 — Evidenced

ACCOUNTABLE OWNER

EVIDENCE / NOTES

7

Business feasibility

Are baseline measurements, implementation costs, review effort and expected value documented?

SCORE ☐ 0 — Not defined ☐ 1 — Partially defined ☐ 2 — Evidenced

ACCOUNTABLE OWNER

EVIDENCE / NOTES

SECTION 02

Decision worksheet

SCORE SUMMARY

DIMENSION	SCORE (0-2)
1. Defined business problem	
2. Data quality and permission	
3. Human accountability	
4. Evaluation criteria	
5. Security and privacy controls	
6. Operational ownership	
7. Business feasibility	
Total (maximum 14)	/ 14

SUGGESTED SCREENING BANDS



These are CCO-designed prompts, not scientific cutoffs or compliance grades.



MANDATORY HOLD

If sensitive-data permissions, human oversight, or critical security controls remain unresolved, do not proceed to live deployment regardless of total score.

DECISION

DECISION	OWNER	DEADLINE
☐ Define prerequisites first		
☐ Run a limited feasibility pilot		
☐ Defer / choose simpler process change		

SECTION 03

Pilot charter

Complete only if appropriate

◆ Workflow boundary and sample users

◆ Baseline metric and desired direction

◆ Human approval point and rollback trigger

◆ Data allowed / excluded

◆ Who reviews exceptions and when

◆ When and how the pilot decision will be made

PILOT SIGN-OFF

REVIEW POINT	OWNER / APPROVAL
Data permission and privacy review	
Human intervention and rollback plan	
Pilot acceptance criteria confirmed	

SECTION 04

Action plan

Record the actions required to close the gaps identified in the readiness review, beginning with any dimension scored 0 or 1 and any item subject to the mandatory hold.

DIMENSION / GAP	ACTION REQUIRED	OWNER	TARGET DATE

NEXT REVIEW DATE

REVIEWED BY

Sources and boundaries

Informed by NIST AI RMF 1.0/Playbook (voluntary risk-management guidance), OWASP 2025 Gen AI application security risks, and the Office of the Privacy Commissioner of Canada. This worksheet does not reproduce or constitute their formal assessment.

- NIST AI RMF Playbook
<https://www.nist.gov/itl/ai-risk-management-framework/nist-ai-rmf-playbook>
- OWASP Gen AI Security Project — LLM Top 10 risks
<https://genai.owasp.org/llm-top-10/>
- Office of the Privacy Commissioner of Canada — Privacy Guide for Businesses (PIPEDA)
https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/pipeda-compliance-help/guide_org/