SENTRAI | GOVERNANCE

Northwind Finance (sample)
ORGANISATION

AI MODEL GOVERNANCE SUMMARY

LOAN DOCUMENT SUMMARISER | NORTHWIND FINANCE (SAMPLE) · LENDING AND OPERATIONS AI

APPROVED v1

EXECUTIVE GOVERNANCE SNAPSHOT

This page summarises the card and highlights where evidence or validation is still needed. The four scores are separate measures and are never combined into one number.

132 / 132
DOCUMENTATION
100% complete

20 / 21
EVIDENCE
95% complete

10 / 21
CONTROL EFFECTIVENESS
48% complete

2 / 2
REGULATORY ASSESSMENT
100% complete

RECORD AT A GLANCE

Attribute	Recorded value	Attribute	Recorded value
Model / record name	Loan Document Summariser	**Record type**	Ai system
Component lifecycle	Released	**Model lifecycle**	Monitoring
Deployment status	Deployed production	**Operational status**	Active
Inherent risk tier	High	**Residual risk tier**	Medium (Assessed)
EU AI Act classification	—	**Korea high-impact**	—
Workflow state	Active monitoring	**Next review**	2027-11-27T15:17:11.226Z (Scheduled)

FRAMEWORK STATUS

Framework (enabled for the organisation)	Automated clause check
NIST AI RMF 1.0	No open gaps (17 met)
ISO/IEC 42001:2023	No open gaps (8 met)

Automated checks and registry mappings; not an assessment, audit or certification.

RISK POSTURE

Inherent High, residual Medium (Assessed). Risk engine: score 11 of 23, score tier High, High with floors. A person sets the tiers; the engine explains and checks them.

KEY GOVERNANCE ATTENTION POINTS

No attention points arise from the card.

1. Finalisation gate

No blockers: the card can be finalised.

Warnings

#	Warning
1	Foundation, parent or fine-tuned-from model is recommended.
2	Embedding dependencies is recommended.
3	Tenants reached is recommended.
4	Tenant notification is recommended.
5	Cross-tenant leakage testing is recommended.
6	Decommissioning date is recommended.

2. Card sections

1. Identity and metadata (15/15 required complete)

Field	Value	Status
Record type *	AI_SYSTEM	Populated · required · entered by a person
Model or record identifier *	NW-AI-0007	Populated · required · entered by a person
Name *	Loan Document Summariser	Populated · required · entered by a person
Provider *	Asterion AI (hosted language model API)	Populated · required · entered by a person
Developer	Northwind Finance, Lending Technology	Populated · recommended · entered by a person
Model category *	LLM	Populated · required · entered by a person
Version *	2.3.0	Populated · required · entered by a person
Release date	2026-08-18	Populated · recommended · entered by a person
Licence	Commercial API licence, enterprise agreement NW-ASTR-2025-11	Populated · recommended · entered by a person
Access type	API	Populated · recommended · entered by a person
Hosting type *	HYBRID	Populated · required · entered by a person
Hosting region *	India (Mumbai)	Populated · required · entered by a person
Deployment identifier	lending-summariser-prod	Populated · recommended · entered by a person
Component lifecycle *	RELEASED	Populated · required · entered by a person
Model lifecycle *	MONITORING	Populated · required · entered by a person
Deployment status *	DEPLOYED_PRODUCTION	Populated · required · entered by a person
Operational status *	ACTIVE	Populated · required · entered by a person
Accountable owner *	0e4c3550-0634-4acb-8262-84b52454853f Refs: nist-ai-rmf-1.0:GOVERN-2, iso-42001-2023:A.3	Populated · required · entered by a person
Technical owner *	1a1a23d1-7cee-4fa4-877b-639306d9c76b	Populated · required · entered by a person
Business owner	00d24767-e6b7-42c6-831e-54ccea94bc1d	Populated · recommended · entered by a person
Registration date	2026-03-02	Populated · recommended · entered by a person
Last updated	2026-11-20	Populated · recommended · entered by a person
Next review date *	2027-05-20	Populated · required · entered by a person

2. Intended use and scope (12/12 required complete)

Field	Value	Status

Field	Value	Status
Business justification *	Underwriters spend about 40 minutes reading the documents attached to each personal-loan application. A structured summary with page references lets them review the file in about 15 minutes without removing their judgement.	Populated · required · entered by a person
Purpose *	Summarises the documents in a personal-loan application (salary slips, bank statements, identity and address proofs) into a structured note for the underwriter. Refs: nist-ai-rmf-1.0:MAP-1, iso-42001-2023:A.6	Populated · required · entered by a person
Intended use *	An underwriter opens an application, requests a summary, and reads it beside the original documents. Every statement in the summary cites the page it came from.	Populated · required · entered by a person
Permitted use *	Use by trained underwriters and credit managers inside the lending workbench, for personal-loan applications in India only.	Populated · required · entered by a person
Observed use	Monitoring of 3,100 sessions shows use matches the intended use; no use outside the lending workbench was found.	Populated · recommended · entered by a person
Intended users *	Underwriters; Credit managers	Populated · required · entered by a person
Affected segments *	Personal-loan applicants Refs: nist-ai-rmf-1.0:MAP-5	Populated · required · entered by a person
Target population	Salaried individuals applying for unsecured personal loans in India	Populated · recommended · entered by a person
Tasks	Document summarisation; Extraction of income and obligation figures with page references	Populated · recommended · entered by a person
Capabilities *	Summarises English and Hindi documents; Extracts stated income, employer and existing obligations; Flags missing or unreadable pages	Populated · required · entered by a person
Languages	English; Hindi	Populated · recommended · entered by a person
Geographic scope *	India	Populated · required · entered by a person
Operating environment	Lending workbench (internal web application), office network only	Populated · recommended · entered by a person
Expected outputs	A one-page structured note with page citations and a list of pages it could not read	Populated · recommended · entered by a person
Decision impact *	SUPPORTS_DECISIONS_ABOUT_PEOPLE	Populated · required · entered by a person
Out-of-scope uses *	Approving or declining an application; Business, secured or credit-card lending; Collections or recovery	Populated · required · entered by a person
Prohibited uses *	Inferring caste, religion, health or other sensitive traits; Producing a credit score or recommendation	Populated · required · entered by a person
Foreseeable misuse	Relying on the summary without opening the source pages; Pasting documents from outside the workbench Refs: eu-ai-act-2024:ART-9	Populated · recommended · entered by a person
Known limitations *	Handwritten documents are often unreadable; Bank statements over 40 pages are summarised in parts; Figures in scanned images below 150 dpi may be misread	Populated · required · entered by a person
Expected performance	At least 97% of extracted figures match the source page on the monthly sample	Populated · recommended · entered by a person
Usage restrictions	Summaries are not stored outside the application file; Not available to third-party agents	Populated · recommended · entered by a person

3. Technical specifications (2/2 required complete)

Field	Value	Status
Architecture description	The workbench sends redacted document text to the provider API with a fixed instruction and a JSON schema, validates the response against the schema, and checks every cited page number exists.	Populated · recommended · entered by a person
Input modalities	Text extracted from PDF and image documents	Populated · recommended · entered by a person

Field	Value	Status
Output modalities	Structured text (JSON rendered as a note)	Populated · recommended · entered by a person
Formats	PDF; JPEG; PNG	Populated · recommended · entered by a person
Inference configuration *	Temperature 0, maximum 1,500 output tokens, JSON schema enforced, no tools, no retrieval, no conversation memory between applications.	Populated · required · entered by a person
Prompts and system prompt *	(sensitive: not printed)	Populated · required · entered by a person
Fine-tuning	None. The provider base model is used as supplied.	Populated · recommended · entered by a person
Runtime	Node.js 22 service in the lending workbench	Populated · recommended · entered by a person
API integration	Calls the provider chat API over a private endpoint with a per-environment key held in the bank key vault.	Populated · recommended · entered by a person
Hosting and deployment architecture	Internal OCR and redaction, provider inference in the Mumbai region, results stored only in the loan application record.	Populated · recommended · entered by a person
Serving technology	Provider-managed API; internal service on Kubernetes	Populated · recommended · entered by a person

4. Data governance and provenance (14/14 required complete)

Field	Value	Status
Training data sources	Not trained by Northwind; provider base model Refs: eu-ai-act-2024:ART-10, iso-42001-2023:A.7	Populated · recommended · entered by a person
Training data period	Not applicable to Northwind (no training)	Populated · recommended · entered by a person
Data ownership	Applicant documents are owned by the applicant and held by Northwind as data fiduciary	Populated · recommended · entered by a person
Data lineage	Application upload, OCR, redaction of account and identity numbers, provider API, schema validation, application record.	Populated · recommended · entered by a person
Data classification *	RESTRICTED	Populated · required · entered by a person
Data quality	OCR confidence is checked per page; pages below the threshold are listed as unreadable rather than summarised.	Populated · recommended · entered by a person
Representativeness	The monthly evaluation sample is stratified by document type, language and branch region.	Populated · recommended · entered by a person
Personal data processed *	YES Refs: gdpr:ART-6, in-dpdp-2023:NOTICE	Populated · required · entered by a person
Personal-data categories *	(sensitive: not printed)	Populated · required · entered by a person
Personal-data flows *	(sensitive: not printed)	Populated · required · entered by a person
Sensitive categories *	(sensitive: not printed) Refs: gdpr:ART-9	Populated · required · entered by a person
Retention *	Prompts and outputs are not retained by the provider (zero-retention setting); summaries are kept with the loan file for 8 years. Refs: in-dpdp-2023:RETENTION	Populated · required · entered by a person
Data residency *	India	Populated · required · entered by a person
Cross-border transfers *	NO Refs: gdpr:ART-44, in-dpdp-2023:CROSS_BORDER	Populated · required · entered by a person
Transfer destination countries *	None	Populated · required · entered by a person
Data minimisation *	Account numbers, identity numbers and signatures are redacted before text leaves Northwind; only the documents of the open application are sent.	Populated · required · entered by a person
Lawful basis or consent *	Consent given in the loan application for processing to assess the application (DPDP Act, s.6) Refs: gdpr:ART-6, in-dpdp-2023:CONSENT	Populated · required · entered by a person

Field	Value	Status
Privacy impact assessment *	https://docs.northwind.example/ai/loan-summariser/privacy-impact-assessment-v2 Evidence: privacy_impact_assessment https://docs.northwind.example/ai/loan-summariser/privacy-impact-assessment-v2; verified by farah.siddiqui@northwind.example Refs: gdpr:ART-35	Verified · required · entered by a person
Copyright and IP	Outputs are owned by Northwind under the provider agreement; no third-party content is reproduced. Refs: nist-ai-600-1:INTELLECTUAL_PROPERTY	Populated · recommended · entered by a person
Data-poisoning assessment	No training or retrieval data is used, so poisoning is limited to the documents of one application; schema and citation checks contain it.	Populated · recommended · entered by a person
Synthetic data	NO	Populated · recommended · entered by a person
Deletion mechanism *	Deleting a loan file deletes its summaries; the provider holds nothing under the zero-retention setting.	Populated · required · entered by a person
Provider may train on inputs *	NO Evidence: provider_terms https://docs.northwind.example/ai/evidence/provider_training_use; verified by farah.siddiqui@northwind.example Refs: nist-ai-600-1:DATA_PRIVACY	Verified · required · entered by a person

5. Dependencies and supply chain (8/8 required complete)

Field	Value	Status
Third-party provider used *	YES	Populated · required · entered by a person
Foundation, parent or fine-tuned-from model	—	Not assessed · recommended
Embedding dependencies	—	Not assessed · recommended
External APIs	Asterion AI chat API	Populated · recommended · entered by a person
Third-party services	Asterion AI (inference)	Populated · recommended · entered by a person
Sub-processors *	Asterion AI cloud hosting (India region)	Populated · required · entered by a person
Open-source libraries and versions	tesseract 5.4; pdf.js 4.2; ajv 8.17	Populated · recommended · entered by a person
SBOM or AI-BOM reference	https://docs.northwind.example/ai/loan-summariser/ai-bom	Populated · recommended · entered by a person
Provider documentation *	https://docs.northwind.example/ai/loan-summariser/provider/asterion-model-documentation-2026 Evidence: provider_documentation https://docs.northwind.example/ai/loan-summariser/provider/asterion-model-documentation-2026; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
SLAs *	99.9% monthly availability; P1 support response within 1 hour	Populated · required · entered by a person
Data processing agreements *	https://docs.northwind.example/ai/loan-summariser/provider/dpa-2025-11 Evidence: contract https://docs.northwind.example/ai/loan-summariser/provider/dpa-2025-11; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Provider certifications *	ISO/IEC 27001; SOC 2 Type II	Populated · required · entered by a person
Third-party risk assessment *	https://docs.northwind.example/ai/loan-summariser/provider/tprm-2026 Refs: iso-42001-2023:A.10, nist-ai-600-1:VALUE_CHAIN	Populated · required · entered by a person
Model update policy *	The model version is pinned. A provider version change needs a regression evaluation and approval by the model owner before it is switched.	Populated · required · entered by a person
End-of-life and deprecation policy	The provider gives 90 days notice of deprecation; the fallback is manual review with no summary.	Populated · recommended · entered by a person

6. Risk classification (10/10 required complete)

Field	Value	Status
Impact severity *	MODERATE	Populated · required · entered by a person
Likelihood *	POSSIBLE	Populated · required · entered by a person
Users reached *	140	Populated · required · entered by a person
Organisations reached	1	Populated · recommended · entered by a person
Tenant reach *	ONE_TENANT	Populated · required · entered by a person
Tenants reached	—	Not assessed · recommended
Autonomy level *	SUGGESTS	Populated · required · entered by a person
Data sensitivity *	HIGH	Populated · required · entered by a person
Reversibility *	REVERSIBLE_WITH_EFFORT	Populated · required · entered by a person
Existing controls	Page citation check on every statement / true / true / https://docs.northwind.example/ai/loan-summariser/tests/citation-check-2026-10; Underwriter reviews source pages before deciding / true / true / https://docs.northwind.example/ai/loan-summariser/audit/underwriter-sample-2026-q3; Redaction before the provider call / true / true / https://docs.northwind.example/ai/loan-summariser/tests/redaction-2026-10	Populated · recommended · entered by a person
Inherent risk tier *	HIGH Refs: nist-ai-rmf-1.0:MAP-4, iso-23894-2023:RISK_PROCESS	Populated · required · entered by a person
Residual risk tier *	MEDIUM Refs: nist-ai-rmf-1.0:MANAGE-1	Populated · required · entered by a person
Risk rationale *	Summaries inform decisions about applicants and contain financial personal data, so harm from a wrong figure is moderate and reversible on review. Residual risk is lower because every statement cites a page, the underwriter checks the source before deciding, and redaction keeps identifiers away from the provider; all three controls were tested in October 2026.	Populated · required · entered by a person
Risk acceptance	Residual risk accepted by the Chief Risk Officer on 2026-11-18	Populated · recommended · entered by a person

7. Impact assessment (8/8 required complete)

Field	Value	Status
Impact assessment *	https://docs.northwind.example/ai/loan-summariser/impact-assessment-v3 Evidence: impact_assessment https://docs.northwind.example/ai/loan-summariser/impact-assessment-v3; verified by farah.siddiqui@northwind.example Refs: iso-42001-2023:A.5, iso-42005-2025:IMPACT_ASSESSMENT	Verified · required · entered by a person
Human and fundamental rights impact *	Applicants could be disadvantaged if a summary understates income. Mitigated by mandatory review of the cited pages and the applicant appeal route.	Populated · required · entered by a person
Privacy impact *	Financial personal data is processed by a provider in India with zero retention; identifiers are redacted. Residual privacy risk is low.	Populated · required · entered by a person
Societal impact	Faster decisions for applicants; no change to who is eligible.	Populated · recommended · entered by a person
Financial impact	A misread figure could lead to a wrong loan amount; caught by underwriter review in the October audit sample.	Populated · recommended · entered by a person
Employment impact	No change to underwriter roles; time saved is used on complex applications.	Populated · recommended · entered by a person
Health and safety impact	None identified.	Populated · recommended · entered by a person
Discrimination impact *	Summary quality could differ by language or document type. Measured monthly; no material gap found.	Populated · required · entered by a person

Field	Value	Status
Vulnerable groups *	First-time borrowers; Applicants with documents in regional languages	Populated · required · entered by a person
Environmental impact	About 1.1 kWh per 1,000 summaries (provider estimate).	Populated · recommended · entered by a person
Stakeholder consultation	Underwriters, the credit policy team and the customer grievance team were consulted in March 2026.	Populated · recommended · entered by a person
Mitigations *	Page citations, mandatory source review, redaction, language-stratified evaluation, appeal route.	Populated · required · entered by a person
Impact assessment approval *	Approved by the AI Risk Committee on 2026-08-12	Populated · required · entered by a person
ISO/IEC 42005 alignment *	The impact assessment follows the structure of ISO/IEC 42005 (scope, affected parties, impacts, mitigations, review). Refs: iso-42005-2025:IMPACT_ASSESSMENT	Populated · required · entered by a person

8. Fairness and bias (7/7 required complete)

Field	Value	Status
Methodology *	Extraction accuracy compared across document language, document type and branch region on a stratified monthly sample of 600 applications. Refs: nist-ai-rmf-1.0:MEASURE-2, nist-ai-600-1:HARMFUL_BIAS	Populated · required · entered by a person
Relevant groups *	Document language (English, Hindi); Branch region	Populated · required · entered by a person
Representativeness	Sample stratified to match the application mix.	Populated · recommended · entered by a person
Metrics *	Extraction accuracy by group; Unreadable-page rate by group	Populated · required · entered by a person
Disparate impact *	Lowest-to-highest group accuracy ratio 0.98 (threshold 0.95) Evidence: bias_test https://docs.northwind.example/ai/evidence/disparate_impact; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Results *	Accuracy 98.1% (English) and 96.9% (Hindi); unreadable-page rate within 1 point across regions. Evidence: bias_test https://docs.northwind.example/ai/evidence/fairness_results; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Mitigation	Hindi OCR model upgraded in July 2026.	Populated · recommended · entered by a person
Residual bias *	A small accuracy gap for Hindi documents remains and is monitored monthly.	Populated · required · entered by a person
Review date *	2026-11-05	Populated · required · entered by a person
Independent evidence	https://docs.northwind.example/ai/loan-summariser/validation/fairness-review-2026 Evidence: independent_review https://docs.northwind.example/ai/loan-summariser/validation/fairness-review-2026; verified by farah.siddiqui@northwind.example	Verified · recommended · entered by a person

9. Explainability and transparency (5/5 required complete)

Field	Value	Status
Explainability methodology *	Every statement cites the source page so the underwriter can check it directly. Refs: nist-ai-rmf-1.0:MEASURE-2	Populated · required · entered by a person
Interpretability	Outputs are short structured statements, each with a source.	Populated · recommended · entered by a person
Explainability limitations	The model does not explain why it chose which details to include.	Populated · recommended · entered by a person
Confidence information *	Pages it could not read are listed; no numeric confidence is shown	Populated · required · entered by a person
Traceability	Each summary stores the prompt version, model version and request id. Refs: eu-ai-act-2024:ART-12	Populated · recommended · entered by a person

Field	Value	Status
User disclosure *	The workbench labels the note "AI-generated summary: check the cited pages". Refs: eu-ai-act-2024:ART-50, kr-ai-basic-act:USER_NOTICE	Populated · required · entered by a person
AI-content labelling *	India / VISIBLE_LABEL / Label on every summary in the workbench Refs: eu-ai-act-2024:ART-50, kr-ai-basic-act:OUTPUT_LABEL, in-it-rules-2026:SYNTHETIC_LABEL, cn-ai-labelling:LABEL	Populated · required · entered by a person
Notification mechanisms	Applicants are told in the privacy notice that AI helps summarise their documents.	Populated · recommended · entered by a person
Appeal and correction *	Applicants can ask for a fresh review by a credit manager through the grievance channel; the summary is not used in that review.	Populated · required · entered by a person

10. Human oversight and accountability (11/11 required complete)

Field	Value	Status
Oversight model *	HUMAN_IN_THE_LOOP Refs: eu-ai-act-2024:ART-14, nist-ai-600-1:HUMAN_AI_CONFIGURATION	Populated · required · entered by a person
Responsible role *	Underwriter (reviews every summary against source pages)	Populated · required · entered by a person
Review frequency	Every use; monthly quality sample	Populated · recommended · entered by a person
Intervention and override	The underwriter can discard the summary and continue without it.	Populated · recommended · entered by a person
Escalation	Errors go to the model owner through the workbench "report a problem" button.	Populated · recommended · entered by a person
Reviewer competency	Underwriters complete the 2-hour AI summary training before access is granted.	Populated · recommended · entered by a person
AI literacy training	Mandatory annual AI literacy module (2026 completion 100%) Refs: eu-ai-act-2024:ART-4	Populated · recommended · entered by a person
Final decision accountability *	The underwriter and credit manager own the credit decision	Populated · required · entered by a person
Automation boundaries	No decision, score or recommendation is produced.	Populated · recommended · entered by a person
Tenant notification	—	Not assessed · recommended
Tools *	None: the assistant has no tools and returns text only	Populated · required · entered by a person
Permissions *	No permissions beyond reading the documents of the open application.	Populated · required · entered by a person
Execution privileges *	None	Populated · required · entered by a person
Autonomous actions *	None	Populated · required · entered by a person
Approval gates *	The underwriter must open the summary; nothing is sent onward automatically	Populated · required · entered by a person
Prohibited actions *	Any write to the loan record other than storing the summary	Populated · required · entered by a person
Transaction limits *	Not applicable: no transactions	Populated · required · entered by a person
Emergency stop *	A feature switch in the workbench turns summaries off for all users within one minute.	Populated · required · entered by a person

11. Evaluation and validation (7/7 required complete)

Field	Value	Status

Field	Value	Status
Evaluation records *	Figure extraction accuracy / ACCURACY / PERIODIC / Stratified sample of 600 applications, two reviewers / 2026-11-05 / Model Validation / Matching figures / 97% / 97.8% / PASS / https://docs.northwind.example/ai/loan-summariser/tests/accuracy-2026-11; Unsupported statements / HALLUCINATION / PERIODIC / 2026-11-05 / Model Validation / Statements without a valid page / < 0.5% / 0.2% / PASS / https://docs.northwind.example/ai/loan-summariser/tests/hallucination-2026-11; Injection in uploaded documents / PROMPT_INJECTION / RED_TEAM / 2026-10-21 / Security Testing / 0 of 120 attacks changed the output format or content / PASS / https://docs.northwind.example/ai/loan-summariser/tests/injection-2026-10 Refs: nist-ai-rmf-1.0:MEASURE-2, eu-ai-act-2024:ART-15	Populated · required · entered by a person
Hallucination evaluation *	https://docs.northwind.example/ai/loan-summariser/tests/hallucination-2026-11 Evidence: evaluation_report https://docs.northwind.example/ai/loan-summariser/tests/hallucination-2026-11; verified by farah.siddiqui@northwind.example Refs: nist-ai-600-1:CONFABULATION	Verified · required · entered by a person
Harmful-output evaluation *	https://docs.northwind.example/ai/loan-summariser/tests/harmful-output-2026-10 Evidence: evaluation_report https://docs.northwind.example/ai/loan-summariser/tests/harmful-output-2026-10; verified by farah.siddiqui@northwind.example Refs: nist-ai-600-1:DANGEROUS_CONTENT	Verified · required · entered by a person
Prompt-injection testing *	https://docs.northwind.example/ai/loan-summariser/tests/injection-2026-10 Evidence: security_test https://docs.northwind.example/ai/loan-summariser/tests/injection-2026-10; verified by farah.siddiqui@northwind.example Refs: nist-ai-600-1:INFORMATION_SECURITY	Verified · required · entered by a person
Cross-tenant leakage testing	—	Not assessed · recommended
Independent validation *	https://docs.northwind.example/ai/loan-summariser/validation/independent-validation-2026 Evidence: validation_report https://docs.northwind.example/ai/loan-summariser/validation/independent-validation-2026; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Red-team exercise *	https://docs.northwind.example/ai/loan-summariser/tests/red-team-2026-10 Evidence: red_team https://docs.northwind.example/ai/loan-summariser/tests/red-team-2026-10; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Next revalidation date *	2027-05-05	Populated · required · entered by a person

12. Security and resilience (5/5 required complete)

Field	Value	Status
Authentication *	Bank single sign-on with multi-factor authentication	Populated · required · entered by a person
Authorisation *	Role-based: underwriter and credit manager roles only	Populated · required · entered by a person
Access control	Access is limited to the open application; no bulk export.	Populated · recommended · entered by a person
API-key and BYOK key management *	(sensitive: not printed)	Populated · required · entered by a person
Encryption at rest	AES-256 in the loan record store	Populated · recommended · entered by a person
Encryption in transit	TLS 1.3 over a private endpoint	Populated · recommended · entered by a person
Prompt-injection protection *	Document text is passed as data inside a fixed schema; instructions in documents are ignored by design and tested quarterly. Refs: nist-ai-600-1:INFORMATION_SECURITY	Populated · required · entered by a person
Model-extraction protection	Per-user rate limit and no public endpoint	Populated · recommended · entered by a person
Adversarial resistance	Quarterly injection and malformed-document tests	Populated · recommended · entered by a person

Field	Value	Status
Poisoning protection	Not applicable: no training or retrieval data	Populated · recommended · entered by a person
Supply-chain security	Pinned dependencies, SBOM, provider assessed annually	Populated · recommended · entered by a person
Vulnerability management	Monthly scans; critical fixes within 7 days	Populated · recommended · entered by a person
Rate limiting	30 summaries per user per hour	Populated · recommended · entered by a person
Abuse prevention	Usage outside working hours is reviewed weekly	Populated · recommended · entered by a person
Incident response *	https://docs.northwind.example/ai/incident-response-playbook	Populated · required · entered by a person
Disaster recovery	Workbench continues without summaries if the provider is down	Populated · recommended · entered by a person
Rollback	Previous prompt version restorable in minutes	Populated · recommended · entered by a person
Business continuity	Manual review is the documented fallback	Populated · recommended · entered by a person
Security assessment evidence	https://docs.northwind.example/ai/loan-summariser/security/assessment-2026-10 Evidence: security_test https://docs.northwind.example/ai/loan-summariser/security/assessment-2026-10; verified by farah.siddiqui@northwind.example Refs: eu-ai-act-2024:ART-15	Verified · recommended · entered by a person

13. Safety and responsible AI (4/4 required complete)

Field	Value	Status
Safety policies	Northwind AI acceptable use policy; Lending AI standard	Populated · recommended · entered by a person
Harm-prevention controls	No recommendation or score is generated; the output is limited to what the documents state.	Populated · recommended · entered by a person
Moderation *	Not needed for document summaries; outputs are schema-validated	Populated · required · entered by a person
Output filtering *	Schema validation and page-citation check on every output	Populated · required · entered by a person
Guardrails *	Fixed instruction, JSON schema, citation check, redaction, no tools.	Populated · required · entered by a person
Misuse prevention	Access only from the workbench; usage reviewed weekly.	Populated · recommended · entered by a person
Dangerous-capability assessment	https://docs.northwind.example/ai/loan-summariser/tests/harmful-output-2026-10 Evidence: evaluation_report https://docs.northwind.example/ai/loan-summariser/tests/harmful-output-2026-10; verified by farah.siddiqui@northwind.example Refs: eu-ai-act-2024:ART-55, nist-ai-600-1:CBRN	Verified · recommended · entered by a person
Robustness safeguards	Large statements split into parts; unreadable pages listed	Populated · recommended · entered by a person
Safety testing *	https://docs.northwind.example/ai/loan-summariser/tests/harmful-output-2026-10 Evidence: evaluation_report https://docs.northwind.example/ai/loan-summariser/tests/harmful-output-2026-10; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Safety incidents	{"state":"ZERO_RECORDED","count":0}	Populated · recommended · entered by a person
Residual safety risk	Low: a wrong summary is caught at review and cannot act on its own.	Populated · recommended · entered by a person

14. Regulatory and legal (6/6 required complete)

Field	Value	Status
Jurisdictions *	IN	Populated · required · entered by a person
India: acts as an intermediary *	NO	Populated · required · entered by a person
Other regulatory classifications	RBI guidance on AI in lending (internal reading) / Decision-support tool / No automated credit decision	Populated · recommended · entered by a person

Field	Value	Status
Applicable laws *	Digital Personal Data Protection Act 2023; DPDP Rules 2025; RBI digital lending directions	Populated · required · entered by a person
Applicability rationale *	Processes personal data of applicants in India and supports lending decisions; not an intermediary; no EU, US or other jurisdiction in scope.	Populated · required · entered by a person
Exemptions	None claimed.	Populated · recommended · entered by a person
Compliance owner *	7bb09eaa-f07e-4c0b-a26c-bc863b729cea	Populated · required · entered by a person
Legal review date *	2026-10-30 Evidence: legal_review https://docs.northwind.example/ai/evidence/legal_review_date; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Next regulatory review	2027-04-30	Populated · recommended · entered by a person

15. Third-party governance (8/8 required complete)

Field	Value	Status
Provider *	Asterion AI Refs: iso-42001-2023:A.10	Populated · required · entered by a person
Provider location *	India (Mumbai region)	Populated · required · entered by a person
Provider documentation *	https://docs.northwind.example/ai/loan-summariser/provider/asterion-model-documentation-2026 Evidence: provider_documentation https://docs.northwind.example/ai/loan-summariser/provider/asterion-model-documentation-2026; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Audit evidence	https://docs.northwind.example/ai/loan-summariser/provider/soc2-2026 Evidence: audit_report https://docs.northwind.example/ai/loan-summariser/provider/soc2-2026; verified by farah.siddiqui@northwind.example	Verified · recommended · entered by a person
Certifications	ISO/IEC 27001; SOC 2 Type II	Populated · recommended · entered by a person
Sub-processors	Asterion cloud hosting (India)	Populated · recommended · entered by a person
Data processing agreement *	https://docs.northwind.example/ai/loan-summariser/provider/dpa-2025-11 Evidence: contract https://docs.northwind.example/ai/loan-summariser/provider/dpa-2025-11; verified by farah.siddiqui@northwind.example	Verified · required · entered by a person
Contractual obligations *	Zero data retention, no training on inputs, India-only processing, 72-hour breach notice, audit rights.	Populated · required · entered by a person
Incident history	One provider outage (47 minutes, 2026-06-03); no data incidents.	Populated · recommended · entered by a person
Change-notification terms *	90 days notice for model deprecation; 30 days for material changes.	Populated · required · entered by a person
Exit strategy *	Switch to the manual process immediately; a second provider has been evaluated and can be onboarded in 6 weeks.	Populated · required · entered by a person
Concentration risk	Single provider for this use; fallback is manual review with no service impact.	Populated · recommended · entered by a person
Responsibility split *	Model behaviour and updates / Asterion AI / Regression test before switching; Redaction and access control / Northwind Lending Technology; Credit decision / Underwriting team	Populated · required · entered by a person

16. Deployment and change management (0/0 required complete)

Field	Value	Status
Environment	Production; UAT	Populated · recommended · entered by a person
Deployment date	2026-08-25	Populated · recommended · entered by a person

Field	Value	Status
Deployment approval	Change CR-2026-0817, approved by the change advisory board	Populated · recommended · entered by a person
Change history	CR-2026-0817 / 2026-08-25 / PROMPT / v13 / v14 / Added page citation requirement / MAJOR / true / AI Risk Committee / false	Populated · recommended · entered by a person
Change-management process	Prompt, model and schema changes go through the bank change process with a regression evaluation.	Populated · recommended · entered by a person
Decommissioning date	—	Not assessed · recommended

17. Monitoring and incidents (10/10 required complete)

Field	Value	Status
Monitored dimensions *	ACCURACY; SAFETY; PRIVACY; FAIRNESS; COST Refs: nist-ai-rmf-1.0:MANAGE-4, eu-ai-act-2024:ART-72	Populated · required · entered by a person
Thresholds *	Accuracy below 97%, unsupported statements above 0.5%, or a group gap above 0.05 opens an incident.	Populated · required · entered by a person
Frequency *	Daily automated checks; monthly sample review	Populated · required · entered by a person
Latest drift status *	Stable (last check 2026-11-26)	Populated · required · entered by a person
Incidents *	{"state":"ZERO_RECORDED","count":0}	Populated · required · entered by a person
Open incidents	{"state":"ZERO_RECORDED","count":0}	Populated · recommended · entered by a person
Incident severity and classification	Severity 1 to 4 per the bank incident standard	Populated · recommended · entered by a person
Affected users	{"state":"ZERO_RECORDED","count":0}	Populated · recommended · entered by a person
Root cause	No incidents recorded.	Populated · recommended · entered by a person
Corrective action	No incidents recorded.	Populated · recommended · entered by a person
Regulatory notification *	Personal-data breaches are notified to the Data Protection Board and affected applicants under the DPDP Rules. Refs: eu-ai-act-2024:ART-73, in-dpdp-2023:BREACH_NOTICE	Populated · required · entered by a person
Grievance channel *	Customer grievance portal and branch grievance officer	Populated · required · entered by a person
Grievances *	{"state":"ZERO_RECORDED","count":0}	Populated · required · entered by a person
Grievance resolution *	Grievances about a decision get a fresh manual review within 15 days.	Populated · required · entered by a person
Suspension criteria *	Accuracy below 95% on any daily check, or any data incident, switches summaries off.	Populated · required · entered by a person
Remediation status	No open remediation	Populated · recommended · entered by a person

18. Environmental sustainability (0/0 required complete)

Field	Value	Status
Inference energy	About 1.1 kWh per 1,000 summaries (provider estimate)	Populated · recommended · entered by a person
Carbon emissions	About 0.8 kg CO2e per 1,000 summaries (provider estimate)	Populated · recommended · entered by a person
Hosting region	India (Mumbai)	Populated · recommended · entered by a person
Efficiency measures	Short fixed instruction and token cap; documents are summarised once per application.	Populated · recommended · entered by a person
Assessment date	2026-10-15	Populated · recommended · entered by a person

3. Risk engine explanation

Score 11 of 23; score tier High; with floors High.

Factor	Value	Points	Note
Impact severity	MODERATE	2/4	—
Likelihood	POSSIBLE	2/4	—
Exposure (tenants and users reached)	ONE_TENANT	1/3	—
Autonomy	SUGGESTS	1/3	—
Data sensitivity	HIGH	2/2	—
Decision impact	SUPPORTS_DECISIONS_ABOUT_PEOPLE	2/4	—
Reversibility	REVERSIBLE_WITH_EFFORT	1/3	—

4. Framework mapping

Where this record supports each framework in the registry. A mapping is not evidence of compliance or certification.

DPDP Act

Applies, date to be confirmed. DPDP Act: obligations mapped to this record (a mapping is not compliance). Registry revision 1, Unverified requires legal review.

Control	Title	Status
NOTICE	Data principals get a notice of what is processed and why	Effectiveness tested (date to be confirmed)
CONSENT	Processing rests on valid consent or a permitted legitimate use	Evidence verified (date to be confirmed)
RETENTION	Personal data is erased when the purpose is served	Effectiveness tested (date to be confirmed)
CROSS_BORDER	Transfers abroad respect any government restriction	Evidence verified (date to be confirmed)
BREACH_NOTICE	Personal data breaches are notified to the Board and the people affected	Effectiveness tested (date to be confirmed)

DPDP Rules

Applies, date to be confirmed. DPDP Rules: obligations mapped to this record (a mapping is not compliance). Registry revision 1, Unverified requires legal review.

ISO/IEC 42001

Applies (organisational standard: this card holds supporting evidence only). ISO/IEC 42001: evidence supporting Annex A controls (organisational standard; this card cannot show conformity). Registry revision 1, Unverified requires legal review.

Control	Title	Status
A.2	Annex A group: policies related to AI	Effectiveness tested
A.3	Annex A group: internal organisation, roles and responsibilities	Evidence verified
A.4	Annex A group: resources for AI systems	Effectiveness tested
A.5	Annex A group: assessing impacts of AI systems	Evidence verified
A.6	Annex A group: AI system life cycle	Effectiveness tested
A.7	Annex A group: data for AI systems	Evidence verified
A.8	Annex A group: information for interested parties	Partially implemented
A.9	Annex A group: use of AI systems	Partially implemented
A.10	Annex A group: third-party and customer relationships	Partially implemented

NIST AI RMF

Applies. NIST AI RMF: practices mapped to this record (a mapping is not compliance). Registry revision 1, Unverified requires legal review.

Control	Title	Status
GOVERN-2	Accountability: roles and responsibilities for AI risk are assigned and documented	Effectiveness tested
MAP-1	Context: intended purpose, setting and expected users are understood and recorded	Evidence verified
MAP-4	Third-party components: risks from external models, data and software are mapped	Effectiveness tested
MAP-5	Impacts: likelihood and size of impacts on people and organisations are characterised	Evidence verified
MEASURE-2	Evaluation: the system is tested for trustworthiness characteristics, with results recorded	Effectiveness tested
MANAGE-1	Treatment: risks are prioritised and a response is decided and recorded	Evidence verified
MANAGE-4	Monitoring: risk treatments, incidents and recovery are monitored after deployment	Effectiveness tested

5. Framework sections

One section for each framework enabled for Northwind Finance (sample) in Governance › Setup. Frameworks that are switched off are not shown. Clause results are automated checks of the recorded model fields at the time of generation.

5.1 NIST AI RMF 1.0

Version	Jurisdiction	Model tier (framework)	Met	Gaps (mandatory)	Not assessed
1.0.0	United States	Standard	17	6 (0)	0

Clause	Requirement	Status	Evidence or gap
GOVERN 2.1	Organizational Ownership & Responsibility	Met	Owner team: Lending Technology
GOVERN 1.2	Board Policy Alignment	Met	Board policy reference: AI-POL-2026
GOVERN 1.5	Audit Cadence Defined	Met	Next audit due: 2027-04-30
MAP 1.1	Purpose & Use-Case Documentation	Met	Use case documented (121 chars)
MAP 1.1	Deployment Context & Affected Users (optional)	Met	Functional area 'lending' affecting segments: Personal-loan applicants
MAP 4.1	Source & Dependency Provenance (optional)	Met	Provenance: northwind/lending/summariser.ts
MEASURE 2.7	Security Red Teaming	Met	Last red teamed 0 days ago (2026-11-27); LOW interval is 365 days
MEASURE 2.4	Performance Drift Measurement	Met	Last drift evaluation 0 day(s) ago
MEASURE 2.3	Performance Benchmarks Recorded (optional)	Met	1 benchmark(s) recorded
GOVERN 3.2	Human Oversight Controls	Met	Human-in-the-loop oversight enabled
MANAGE 2.4	Fallback / Business-Continuity Plan (optional)	Gap	High-risk models need a configured business-continuity fallback (activate via /monitoring/bcp).
MANAGE 4.3	Incident Reporting Hygiene	Met	No overdue incident reports
MANAGE 2.1	Risk Response Resourcing	Met	Risk response owned by Lending Technology
MEASURE 3.1	Risk Tracking Mechanisms	Met	346 ledger event(s) tracking this model over time
MEASURE 2.10	Privacy Risk Examined (DPIA / Privacy Review)	Met	DPIA / privacy-review artifact attached
MANAGE 1.3	Risk Responses Planned and Documented (Risk Register) (optional)	Gap	Map and Manage need identified risks with likelihood and impact: record and assess this system's risks.
MAP 3.2	Context Profile: Costs of Errors, Limitations and Out-of-Scope Uses (optional)	Gap	Map stage needs the system's context documented in structured form: complete the context profile.
GOVERN 6.1	Third-Party Risk Policies Applied (optional)	Met	No third-party components recorded
MEASURE 2.6	Safety Re-evaluated After Risk Escalation (optional)	Met	No red-team exercise outstanding
MEASURE 2.13	Effectiveness of TEVV metrics evaluated (optional)	Gap	Register test sets with acceptance criteria for the system.
MANAGE 4.3	Incidents communicated to relevant AI actors (optional)	Met	—
MEASURE 2.12	Environmental impact and sustainability assessed (optional)	Gap	Record the system's energy use (kWh) and CO2e.
MEASURE 2.7	AI system security and resilience evaluated (attack categories) (optional)	Gap	Approve an AI threat model for the system (state: NONE).

5.2 ISO/IEC 42001:2023

Version	Jurisdiction	Model tier (framework)	Met	Gaps (mandatory)	Not assessed
2023.1.0	International	Standard	8	10 (0)	1

Clause	Requirement	Status	Evidence or gap
6.1.2	AI System Risk Assessment	Met	System evaluated risk tier: LOW
8.4	AI System Impact Assessment (6.1.4 / 8.4) (optional)	Gap	Clauses 6.1.4 and 8.4 require a signed AI system impact assessment: complete and finalise one for this model.
A.7.5	Data & Codebase Provenance	Met	Source/data references tracked: northwind/lending/summariser.ts
9.1	Performance Monitoring & Measurement (optional)	Met	Last drift evaluation 0 day(s) ago
9.2	Internal Audit Cadence (optional)	Met	Next audit scheduled for 2027-04-30
10.2	Nonconformity & Corrective Action (optional)	Met	No overdue incident reports
5.3	Roles, Responsibilities & Accountability	Met	Accountable team assigned: Lending Technology
A.6.2.7	AI System Technical Documentation (optional)	Gap	Annex A.6.2.7 recommends technical documentation for relevant parties (attach a model_card artifact).
6.1.3	AI Risk Treatment (Risk Register) (optional)	Gap	Clauses 6.1.2–6.1.3 and 8.2–8.3 need an assessed risk register: record and assess this system's risks.
A.6.2.2	AI System Requirements and Specification (optional)	Gap	Annex A.6.2.2 needs the system's requirements and intended use specified: complete the context profile.
A.8.2	System Documentation and Information for Users (optional)	Gap	Annex A.8.2 needs information for users, including limitations: complete the context profile.
A.10.3	Suppliers (optional)	Met	No third-party components recorded
A.7.2	Data for Development and Enhancement (optional)	Gap	A.7 needs the data used by the system defined and documented: link its datasets.
A.6.2.4	Verification and Validation (optional)	Gap	A.6.2.4 needs verification and validation of the system recorded.
A.6.2.4	Verification and Validation (test sets) (optional)	Gap	Register test sets with acceptance criteria for the system.
A.8.4	Communication of Incidents (optional)	Met	—
A.5.5	Societal Impacts (environmental) (optional)	Gap	Record the system's energy use (kWh) and CO2e.
A.6.2.6	Operation and Monitoring (AI security) (optional)	Gap	Approve an AI threat model for the system (state: NONE).
A.10.4	Customers (optional)	Not assessed	—

6. Approval history

Decided	Step	Decision	By	Comment and conditions
2026-11-27	**Governance**	Approved with conditions	daniel.dsouza@northwind.example (Approver)	Approved for production use in lending. Condition: Re-run the Hindi accuracy test after the next OCR upgrade (owner ravi.iyer@northwind.example, due 2027-02-28)
2026-11-27	**Risk**	Approved	farah.siddiqui@northwind.example (Ciso)	Residual risk within appetite; controls tested.
2026-11-27	**Final**	Approved	farah.siddiqui@northwind.example (Ciso)	Final approval.

7. Document control

Attribute	Value
Status	APPROVED v1
Workflow state	Active monitoring
Organisation	Northwind Finance (sample) · Lending and operations AI
Record ID	ecaf62c0-fba2-421f-9168-84c81e8494e0
Content hash (SHA-256)	edd30993a343b51bd10979c25d9541efc10f2128d7032e0ae88c3fc78ab94834
Generated	2026-11-27T15:17:14.544Z by asha.menon@northwind.example
Catalogue version	2.0.0

This model card documents the system. Framework mappings are not evidence of compliance or certification.

A model card is a documentation and transparency artefact. It is not, by itself, proof of regulatory compliance, certification, or conformity of an organisation's AI management system.