NAICAS Evidence Requirements Guide

Operational submission requirements for certification applications.

Document Classification	Public Evidence Guide (Operational Submission Requirements)
Authority Level	Non-amending guide (Rulebook governs)
Version	1.0
Effective Date	2025-12-01
Contact	info@naicas.org

1. Submission overview

- Submit one application per AI model or materially distinct workflow.
- Select the certification level (L1-L4) that matches the workflow authority.
- Provide an evidence package that is complete, readable, and internally consistent.
- Submit documents as PDFs. Remove or redact sensitive personal data (NPPI/PII) unless explicitly required.
- Include a Submission Index that lists every artifact, version, and owner.

2. Recommended submission package structure

Provide a single ZIP (or folder) with an index and consistent filenames.

- 00_Submission_Index.pdf (table of contents + version list)
- 01_Scope_Declaration.pdf
- 02_System_Overview.pdf
- 03_Control_Matrix.pdf
- 04_Disclosure_Library.pdf
- 05_Safety_and_Escalation.pdf
- 06_Logging_and_Auditability.pdf
- 07_Data_Handling_and_Retention.pdf
- 08_Change_Management.pdf
- 09_Testing_and_Validation_Summary.pdf

- 10_Level_Specific_Artifacts.pdf (or subfolder)
- 11_Attestations_and_Signoff.pdf (role-based signoff)

3. Minimum evidence set (all levels)

The following artifacts form the baseline submission package for every level.

Evidence artifact	What it demonstrates	Minimum contents
Scope Declaration	Exactly what the AI can do and cannot do	Workflow description; user types; allowed actions; prohibited actions; integrations; out-of-scope scenarios.
System Overview	How the system works at a high level	Architecture diagram; model(s) used; inputs/outputs; dependencies; environments; key controls.
Compliance Control Matrix	Traceable mapping from requirements to controls	Requirement -> control -> evidence -> owner -> frequency.
Disclosure Library	Standard language used in interactions	Identity disclosure; limitations; consent language; notice language (where applicable).
Safety & Escalation Controls	Human oversight and safe failure behavior	Escalation triggers; handoff method; kill switch; fallback handling; high-risk category handling.
Logging & Auditability	Reconstruction of actions and decisions	Log schema; correlation identifiers; retention; access controls; sample redacted logs.
Data Handling & Retention	Proper handling of consumer data	Data categories; storage locations; minimization; retention schedule; deletion process.
Change Management	How updates are controlled	Versioning; approvals; rollback; monitoring after release; material-change definition.
Testing & Validation Summary	Evidence that behavior has been evaluated	Test plan; scenario coverage; results summary; known limitations; remediation actions.
Attestations & Signoff	Accountability for submitted evidence	Signoff for scope, disclosures, security controls, and operational ownership.

4. Level-specific evidence

Add the following level-specific artifacts in addition to the baseline evidence set.

Level	Add these artifacts (in addition to baseline)
Level 1 (Data Intake)	Sample intake flows (scripts/forms); sample transcripts (redacted); disclosure/consent capture evidence (where applicable).

Level	Add these artifacts (in addition to baseline)
Level 2 (Quoting)	Quote/rating workflow diagram; sample quotes (redacted); premium explanation templates; notice mapping by jurisdiction (if applicable).
Level 3 (Binding & Application)	Binding authority controls and permission model; payment handling flow and safeguards (if applicable); sample application/binding packet (redacted); underwriting escalation rules and exception handling.
Level 4 (Full Operations)	End-to-end workflow map; monitoring plan (drift, incident response, enforcement actions); recertification triggers and operational change thresholds; rollback/kill switch procedures and responsibilities.

5. Evidence quality rules

- Every requirement in the Control Matrix must point to a specific evidence artifact and section.
- Evidence must be internally consistent (names, versions, workflow scope).
- Provide timestamps or effective dates for policies and procedures.
- Provide a clear owner for each control (role or function; individual names optional).
- Use stable identifiers (system name, system version, workflow name) consistently across all artifacts.

6. Artifact guidance

These points describe what reviewers expect to see in common artifacts.

6.1 Scope Declaration

- One-page summary at the top: what the system does, who uses it, and what it outputs.
- Explicit prohibited actions (for example, binding without authority; collecting data outside approved scope).
- Out-of-scope scenarios and escalation triggers.

6.2 System Overview

- Diagram of components and data flow.
- Major dependencies and failure modes.
- How prompts, rules, and policies are versioned.

6.3 Control Matrix

- Minimum columns: Requirement, Control, Evidence Reference, Owner, Frequency, Status.
- Evidence references should include filename and section/page.

6.4 Disclosure Library

- Channel-specific variants (web, SMS, voice, email) where applicable.
- Mapping between workflow stages and disclosure moments.

6.5 Logging & Auditability

- Define what is logged, when it is logged, and what identifiers are used.
- Provide a sample of redacted logs sufficient to reconstruct a single workflow run end-to-end.

7. Redaction and confidentiality

- Remove or redact NPPI/PII from samples (transcripts, logs, screenshots) unless explicitly required.
- If evidence includes real data, describe the redaction method and fields removed.
- Do not include live credentials, API keys, secrets, or raw database connection strings.

8. Submission Index template

Include an index table with at least the fields below.

Field	Description
Artifact Name	Human-readable artifact name (for example, System Overview).
Filename	Exact filename included in the submission package.
Version	Artifact version identifier.
Owner	Role or function responsible for the artifact.
Effective Date	Policy/procedure effective date where applicable.
Notes	Optional notes on scope or applicability.

9. Common deficiency triggers

- Scope is ambiguous or changes across documents.
- Disclosures do not match the workflow channel or authority level.
- Logs cannot reconstruct actions, outputs, and notices.
- Change management does not define material changes or rollback procedures.
- Level-specific artifacts are missing for requested authority.

10. Pre-submit checklist

- Scope is explicit and matches the requested level.
- Control Matrix links to every artifact.
- Disclosures match the workflow and channel.
- Logging examples are readable and correspond to the workflow.
- Version identifiers are present on all artifacts.
- Submission Index lists all artifacts and owners.