NAICAS Certification Application Packet - Submission Checklist - v1.0

National Association of Insurance & Compliance for AI Systems (NAICAS)

Document Classification: Application Packet (External-Facing; Operational Submission Requirements)
Authority Level: Operational Requirements (Non-Rulebook; Non-Amending)
Version / Effective Date: 1.0 / December 1, 2025
Issued By: NAICAS Governance Committee + Technical Standards Council
Contact: info@naicas.org | NAICAS.org

Non-Binding Notice (Standards Control)

- This packet defines submission and completeness requirements for NAICAS certification applications.
- It does not create, amend, supersede, or reinterpret NAICAS standards, certification requirements, scoring thresholds, enforcement authority, or regulatory alignment obligations.
- Certification decisions remain evidence-based and governed by the NAICAS Rulebook and applicable certification procedures.
- Payment of fees does not guarantee certification approval.

Purpose of this packet

This packet standardizes certification submissions to ensure:
- Scope clarity
- Evidence completeness
- Review discipline
- Auditability
Incomplete or inaccurate submissions will not be reviewed until corrected.

1) General requirements (all applicants)

Before submission, the applicant MUST:
- Read and understand the purpose of this packet.
- Ensure the submission is complete and accurate.
- Understand that certification does not guarantee carrier acceptance.
- Acknowledge that certification may be suspended or revoked.
- Acknowledge that fees do not influence outcomes.
Submission format requirements:
- Submit all materials in PDF format unless explicitly permitted otherwise by NAICAS.
- Redact sensitive personal data from all submitted materials.
- Label files clearly (see File Naming Standard).
- Submit through the NAICAS-designated intake channel only.
Data handling requirement:
- Applicants MUST NOT submit unredacted sensitive personal data (SSNs, full payment card numbers, full driver's license numbers, etc.) unless explicitly requested by NAICAS under secure procedures.

2) Certification scope (single model or distinct workflow)

The application MUST be for:
- A single AI model, OR
- A materially distinct AI workflow
Rules:
- Each model or workflow must be submitted separately.
- If a system contains multiple materially distinct workflows, each workflow requires its own application packet.
- Scope expansion after certification requires recertification under NAICAS procedures.

3) Certification level selection (select one)

- Level 1 - Data Intake Compliance
- Level 2 - Quoting Compliance
- Level 3 - Binding and Application Compliance
- Level 4 - Full Operational Compliance
Note: scope expansion requires recertification.

4) Section A - Applicant information (required)

[ ] Legal Entity Name
[ ] DBA (if applicable)
[ ] Primary Contact Name
[ ] Primary Contact Title
[ ] Primary Contact Email
[ ] Primary Contact Phone
[ ] AI System Name
[ ] Current Version
[ ] Hosting Environment (Cloud / On-Prem / Hybrid)

5) Section B - Scope declaration (required)

Clearly define system boundaries. Minimum required scope fields:
[ ] Lines of business supported
[ ] States of operation
[ ] Carrier interaction type (read / quote / bind)
[ ] Payment handling (if applicable)
[ ] Human oversight model (required)
Attestation:
- Applicant MUST attest that the declared scope is complete and accurate.

6) Section C - Required documentation (all levels)

Submit the following documents for all levels:

Doc code	Document	Must include
C-1	System Overview Document	- Architecture summary - Functional scope - AI role definition
C-2	Compliance Control Matrix	- Mapping of controls to NAICAS requirements (Rulebook references)
C-3	Disclosure Language Library	- All consumer-facing disclosures (compiled) - State-specific notice handling description (if applicable)
C-4	Escalation and Safety Controls Description	- Human handoff logic - Hard-stop conditions
C-5	Logging and Auditability Documentation	- Logged fields inventory - Retention policy statement - Access controls summary
C-6	Change Management Policy	- Update notification process - Drift detection controls - Evidence of version tracking process

7) Section D - Level-specific requirements (required based on level selected)

Level 1 - Data Intake Compliance

[ ] D1 - Intake workflow diagram
[ ] D2 - Sample intake transcripts (redacted)

Level 2 - Quoting Compliance
[ ] D3 - Rating engine integration description
[ ] D4 - Sample quotes (redacted)
[ ] D5 - Required notices delivery proof (how and when notices are delivered)

Level 3 - Binding and Application Compliance
[ ] D6 - Binding workflow diagram
[ ] D7 - Payment authorization flow
[ ] D8 - Sample application packet (redacted)

Level 4 - Full Operational Compliance
[ ] D9 - End-to-end lifecycle map
[ ] D10 - Continuous monitoring documentation
[ ] D11 - Multi-state logic handling (if multi-state)

8) Section E - Attestations (required)

Applicant MUST sign and date all attestations. Attestation set (minimum required):
[ ] Accuracy of submitted materials
[ ] Scope adherence commitment
[ ] Monitoring cooperation agreement
[ ] Enforcement acceptance
[ ] Certification revocation acknowledgment
Authorized signatory (required fields):
[ ] Authorized Signatory Name
[ ] Title
[ ] Signature
[ ] Date

9) File naming standard (required)

All files MUST be labeled clearly using this format:
NAICAS_[ORGNAME]_[SYSTEMNAME]_[LEVEL]_v[VERSION]_[DOC-CODE]_EFFECTIVE-2025-12-01.pdf

Examples	Filename
Disclosure library	NAICAS_AcmeAI_RateBot_L2_v3.2_C3-Disclosure-Library_EFFECTIVE-2025-12-01.pdf
Payment flow	NAICAS_AcmeAI_RateBot_L3_v3.2_D7-Payment-Flow_EFFECTIVE-2025-12-01.pdf

Document codes:
- Section C documents: C-1 through C-6
- Section D documents: D1 through D11
- Attestations: E-Attestations

10) Review process (informational)

The review process steps are:
- Intake completeness check
- Documentation review
- Scenario testing
- Scorecard evaluation
- Certification determination
- Registry listing (if approved)