NAICAS Rulebook v1.0 - Public Requirements and Evidence Checklist

Version: 1.0 | Effective Date: 2025-12-01 | Next Scheduled Review: 2026-12-01

1. Authority and scope

This document consolidates the practical requirements and evidence expectations for NAICAS certification. It is intended for vendors, agencies, carriers, reviewers, and other stakeholders.

Normative language

- MUST / SHALL = mandatory
- MUST NOT / SHALL NOT = prohibited
- SHOULD = recommended
- MAY = permitted

2. What is covered

- AI models, AI agents, and automated workflows used in auto insurance operations.
- Consumer-facing interactions and operational decision-making that affects eligibility, pricing, coverage terms, or transaction processing.
- Deployments by agencies, carriers, MGAs, vendors, and similar entities operating in U.S. auto insurance contexts.

3. Certification levels

Level	Authorized scope	Not permitted
Level 1 - Data Intake	Collect and validate consumer-provided data; deliver required disclosures.	Quoting, presenting premium amounts, binding, payments, application submission.
Level 2 - Quoting	Generate, present, and explain premium quotations within carrier and state rules.	Binding, payments, application submission.
Level 3 - Binding and Application	Bind coverage within approved authority; process payments; submit applications.	Operating outside carrier authority; skipping mandatory escalation.
Level 4 - Full Operational	End-to-end autonomous workflows within defined boundaries and continuous monitoring.	Operating outside law, carrier rules, or escalation requirements.

4. Core principles reviewers will test

- Accuracy: outputs match approved carrier rules and verified sources.
- Identity and disclosures: AI identity, scope, and required notices are delivered consistently.
- Compliance: state and carrier rules are followed; stricter carrier rules prevail.
- Safety: mandatory human escalation triggers are enforced.
- Auditability: logs and records support reconstruction of interactions and decisions.
- Reliability: behavior remains stable across changes; drift is detected and addressed.

5. Evidence package - what to submit

Submit one package per AI model or materially distinct workflow. Provide the items below in labeled PDFs.

A. Scope and system description

- Scope declaration: what the system is allowed to do, by level (L1-L4).
- Workflow diagrams: intake, quote, bind, handoff, and failure paths.
- Integration map: carriers, rating engines, payment processors, document delivery mechanisms.

B. Consumer communication and disclosures

- AI identity disclosure language and placement.
- Required notices: privacy, data use, non-binding quote disclaimers, and state-specific notices.
- Coverage explanation and premium explanation templates.

C. Controls and safety

- Escalation policy: trigger list, handoff method, and escalation logging.
- Hallucination prevention controls: boundaries, grounding, and failover behavior.
- Error handling: hard-stops for missing disclosures, incomplete data, and payment failures.

D. Data handling and security

- Data intake rules: structured questions, confirmation of inputs, conflict detection and resolution.
- Access controls and retention policy for logs and evidence.
- Privacy compliance approach and safeguards for nonpublic personal information.

E. Auditability and monitoring

- Logging specification: transcripts, disclosures delivered, consents, quote/bind events, and version context.
- Immutable records approach and retention period.
- Monitoring plan: drift detection, regression testing, and incident response.

F. Change management

- Release process and approval controls for model updates and prompt/workflow changes.
- Notification procedure for material changes affecting system behavior.

6. Level-specific evidence add-ons

- Level 1: intake transcript samples and disclosure delivery proof.
- Level 2: quote generation proof, rating engine alignment evidence, and state notice delivery proof.
- Level 3: binding authority boundaries, payment flow controls, and application packet examples.
- Level 4: continuous monitoring plan, regression testing suite summary, and drift response runbook.

7. Review outcomes and ongoing obligations

- Monitoring and audits may be required throughout the certification period.
- Recertification may be triggered by model updates, workflow changes, carrier rule changes, or regulatory changes.
- Violations can result in corrective actions, suspension, or revocation.

Contact: info@naicas.org | NAICAS.org