

AUDIRA: PRE-LAUNCH VALIDATOR SPEC

Version: 1.0

Purpose: Define the automated validation module that ensures every AI agent deployed through Audira is complete, compliant, functional, and simulation-tested before activation.

Overview

The Pre-Launch Validator is a backend module that runs **automatically** after onboarding completion. It validates whether the agent is:

- Fully configured across discovery dimensions
- Behaviorally sound under simulated user interactions
- Technically and legally ready to launch

If any condition fails, the platform halts launch and shows a smart alert with remediation guidance.

Validation Categories & Criteria

1. Tag Completion Check

Rule	Description
All 10 core discovery tags must be populated	Either by onboarding answers, dynamic responses, or uploaded documents
Tag source must be traceable	System logs must show whether tag came from fixed, dynamic, or fallback response
Manual override (admin-only)	Only allowed for enterprise accounts via secure console

2. Simulation Score Threshold

Audira simulates 5–7 test interactions and scores:

Metric	Description	Pass Threshold
Tone Match	Matches defined tone settings	≥90%
Intent Routing	Correctly identifies user intent	≥90%
Fallback Handling	Properly responds to unknowns	≥90%
Escalation Behavior	Redirects to human or correct flow	≥90%
Overall simulation must average ≥90%. Any metric <85% triggers mandatory deep-dive reconfiguration.		

3. Blueprint & Config Completeness

Asset	Required Content
agent_config.json	Tone, persona, tags, use-case config, fallback behavior
Agent Blueprint.pdf	Business summary, tag logic, tone settings, integrations, sample messages
Training data manifest	If RAG used, document sources and structure must be listed

4. Compliance Risk Scan

Trigger	Response
Compliance tag (#compliance_constraints) active	Validator checks for region-specific rules
Missing consent fallback	Auto-fail with remediation alert
PII markers in training data	Alert + human review required

5. Integration Auth & Readiness

Scenario	Requirement
Integration tag active but no API key/token provided	Block go-live + request credential setup
Webhook-based trigger selected	Test ping to endpoint before approval
Booking/CRM integration selected	Must pass dry-run test with sandbox or dummy data

Smart Alerts & Remediation Flow

If validation fails, platform shows:

- Problem summary (e.g. "Tone mismatch on 2 test queries")
- Affected tag(s)
- Suggested fix (reconfigure tone, upload fallback logic, connect API)
- Action button to resolve or revisit onboarding

All alerts are logged and included in audit trail per agent version.

Logging & Audit

- Each validation cycle generates a session log
 - Hash-stamped for traceability
 - Tracks version of config, tags, simulation prompts, and results
 - Retained per account for up to 2 years (GDPR-compatible)
-

Optional Manual Review Layer

- Enterprise clients or flagged verticals (e.g., healthcare, finance) may be routed to a consultant
- Manual review is logged with notes and overrides
- Reviewer must sign off on risk exceptions

 **Final Launch Trigger**

Once all 5 categories are validated:

- Agent status set to launch_ready: true
 - Go Live button becomes active
 - JSON config and PDF downloadable
 - Simulation preview is unlocked for team review
-

Next Document: Agent Blueprint Template