

Our Validation Approach

Status: Published, [Secureframe Link](#)

Published date: July 29, 2026

Last updated: July 29, 2026

Policy owner: Anatoly Geyfman

How Deviceflow follows industry best practice for risk-based, continuous, and audit-ready software assurance, per GAMP 5 Second Edition guidelines.

A note on validation

Deviceflow sits between the medical device field and your systems of record — ingesting emails, charge sheets, inventory notices, and rep activity, and writing structured data into ERPs, billing systems, and partner networks.

Because we touch information that flows directly into orders, inventory, and invoices for implantable devices, your quality and compliance teams need confidence that the system does what it says it does, every time.

The shift from **validation** to **assurance** in the FDA's 2022 Computer Software Assurance (CSA) draft guidance encourages vendors like us to carry the bulk of the testing weight, leaving customers to focus on the risks specific to their own business processes.

This document explains how we've applied that best practice — and how we share the validation work with you.

What is computerized system validation (CSV)?

The FDA defines validation as the confirmation by examination of objective evidence that software specifications conform to user needs and intended uses, and that requirements implemented through software can be consistently fulfilled.

CSV answers one question: **Is your software fit for your intended use in a regulated GxP environment?**

For Deviceflow's customers, that question has real weight. When our platform ingests a Bill-Only purchase order from a sales rep's email and writes it into your ERP, the data flowing through that pipeline determines what gets billed, what gets replenished, and which devices end up in the next surgical case.

What is computerized system assurance (CSA)?

The FDA's 2022 CSA draft guidance emerged as a corrective to legacy CSV frustrations:

1. **Redundant validation tasks** performed by the customer out of fear of regulatory punishment.
2. **Reliance on outdated artifacts** like IQs, OQs, and PQs that don't reflect modern, continuously-released software.
3. A general perception of validation as a time-consuming, paper-heavy process.

The terms "validation" and "assurance" are used interchangeably. What changes is where the work lives.

CSA shifts the work to the vendor. Deviceflow performs system-level testing continuously using automated test suites and recorded evidence. You inherit that work. Your focus narrows to the configurations and business processes your team has built on top of the platform.

Deviceflow's GAMP category

Deviceflow is a multi-tenant SaaS platform with significant per-customer configuration: account hierarchies, rep certification rules, ERP integration mappings, document parsing templates, partner routing logic, and order workflows are all configurable. Because of this configuration surface, Deviceflow is classified as **GAMP Category 4 — Configured Software Product**.

Category 4 sits between Category 3 (fixed off-the-shelf software) and Category 5 (custom-coded systems). GAMP 5 Second Edition (ISPE, July 2022) defines a risk-based onboarding model for Category 4 products that we follow: internal risk assessment, requirements driven by user needs, configuration specifications, functional risk assessment, and test coverage that traces back to requirements.

Risk classification

Deviceflow does not directly manufacture, label, or release devices. Because we orchestrate data that affects which devices reach patients — and may handle regulated identifiers in case records — Deviceflow is classified as a **medium-risk** system.

Level	Description
High	Directly impacts product quality or human safety. Could cause or impede a product recall.
Medium	Deviceflow is here. Required for regulatory compliance (audit trail integrity). Indirectly impacts product quality or human safety.
Low	Business risk only.

How our assurance approach works

Validation is a shared exercise. Most of the work is performed by Deviceflow as your vendor.

What Deviceflow provides

- Maintains and operates the Deviceflow platform.
- Maintains a documented software development lifecycle (SDLC) and quality practices.
- Documents user needs, user stories, and the functional behavior built to satisfy them.
- Performs continuous, automated system testing on every release and publishes the results at validation.deviceflow.com.
- Provides a versioned validation pack — requirements, tests, evidence — for every release.

What you (the customer) provide

- Manage your configuration and data inside Deviceflow.
- Use Deviceflow's documentation to evaluate alignment with your needs.
- Document your business processes and the risks Deviceflow touches.
- Perform any additional configuration-specific testing your risk assessment requires.
- Maintain your own validation summary and audit evidence inside your QMS.

You do not need to re-create documents for user needs, functions, or system-level testing. Those are covered by Deviceflow. What you document is your business risk picture and how you've configured Deviceflow against it.

End-to-end assurance process

1. Supplier qualification

We maintain a completed Vendor Questionnaire covering company information, quality practices, SDLC, change management, security, backup and recovery, data integrity, support, and validation support. We support remote supplier audits.

2. Planning

A Validation Plan lays out your customer-specific approach: what's in scope, your GxP determination, and what testing you'll perform on top of Deviceflow's inherited validation pack.

3. Business requirements and risk assessment

You document the business processes Deviceflow touches (order intake, charge capture, inventory, billing) and rank the risks Deviceflow introduces or mitigates. This scopes any configuration-specific testing.

4. Requirements, testing, and traceability

User requirements, the functions built to meet them, and the tests executed against them are all maintained in our SDLC and published with every release. The validation pack includes:

- **Requirements Traceability Matrix (RTM)** — links each user need to the user story to the automated test.
- **Test Plan** — automated test scripts, passing results, and execution timestamps.
- **User Needs** — the requirements list scoped to the release.
- **Test evidence** — browser-based automated tests (Playwright/Chromium) executing against a real environment. Each test produces step-by-step screenshots, video recordings, database audit log verification, and structured pass/fail results.

All validation evidence is published at validation.deviceflow.com. The site is built with Astro/Starlight and maintains a complete, browsable archive of every release version.

5. System configuration

Customers receive onboarding support to document their Deviceflow instance configuration. This becomes the baseline for change control going forward.

6. Validation Summary Report (VSR)

Summarizes the validation effort and the system's fitness for use. Authorizes release of Deviceflow into your production GxP environment.

Re-assurance and change management

Every change we ship is tested before release and published in the next version of our validation pack. Deviceflow ships on a roughly weekly cadence. Validation is not a separate activity — it is tied to the release.

Each release is identified by date and Git commit SHA (e.g., `2026-04-20-d326c2b`) and is accompanied by:

- A change history per feature area.
- Updated requirements traceability for any modified requirements.
- Re-executed automated tests with fresh evidence.
- A versioned snapshot of the validation site so prior releases remain auditable.

Your job is to assess the impact of each release on your configuration and documented business processes. Most releases are small, incremental enhancements. Material changes are flagged in advance.

When re-validation is triggered

- The way you use Deviceflow changes in a way that affects your risk analysis.
- A new Deviceflow feature affects your risk analysis.
- A significant version is rolled out.

Your Quality Manager determines if and when re-validation is needed.

Attestation

I attest that the information provided in this document is accurate and complete to the best of my knowledge.

Field	Value
Name	Anatoly Geyfman
Title	CEO
Signature	
Date	07/29/2026

FAQs

If Deviceflow tests the software, do I still need to test it? Deviceflow runs identically for every customer. Repeating our system-level tests is redundant. Your testing is scoped to the configurations unique to your business — ERP mappings, account rules, partner routes, rep policies. The FDA's CSA guidance encourages this risk-based, least-burdensome approach.

Why don't you provide IQ, OQ, and PQ documents? IQ/OQ/PQ artifacts were designed for installed software with a discrete go-live event. They don't fit a continuously-released SaaS platform. Both FDA CSA guidance and GAMP 5 Second Edition have moved away from this model. We provide test scripts,

requirements, and execution evidence that your team can reformat to internal templates if needed.

What if my auditor wants a more traditional package? Our artifacts — User Needs, User Stories, RTM, Test Plans, and execution evidence — contain everything an auditor needs. We support customers through the audit process.

How do I see the test evidence? Every release publishes a versioned validation site at validation.deviceflow.com containing the RTM, test reports, screenshots, videos, and assertions for every requirement. Past releases remain accessible so prior states stay auditable.

What regulations and guidelines do you follow? 21 CFR Part 11 (Electronic Records), EudraLex Volume 4 Annex 11 (Computerised Systems), ISPE GAMP 5 Second Edition (July 2022), PIC/S PI 011-3, and the FDA's 2022 Computer Software Assurance draft guidance.

For more information, visit deviceflow.com or contact us directly.