azumuta

FOR QA, VALIDATION AND IT TEAMS

GMP documentation pack

Five short documents that answer the first questions your quality team asks about a new system in a GMP environment. Read them before a demo, or pass them on to your validation lead.

1 **Working with Azumuta as a GMP supplier**
What you can expect from us, at a glance

2 **21 CFR Part 11 and Annex 11 capability overview**
Which controls the platform has

3 **How validation works with Azumuta**
Who does what, deliverable by deliverable

4 **Release and change summary**
How updates reach a validated system

5 **Hosting, security and continuity**
Where it runs, how data is protected, what if the network drops

Informational. Binding terms live in the Quality Agreement, the on-premise SLA and the License Terms.

DOCUMENT 1

Working with Azumuta as a GMP supplier

You run Azumuta from the same codebase as every other customer, installed on your own infrastructure under a controlled, documented model. Here is what that means for your quality team.

One product, your GMP configuration

There is one Azumuta product, used for many use cases and in many sectors. You get it as a containerised package from our single codebase and run it yourself, with a GMP configuration that you control.

You decide when to upgrade

Every release comes with its full documentation set and changelog. You choose which releases to take and which to skip.

What ships with every release

- Release notes where every change carries its category, impacted module, GMP impact level and links to its requirement and test
- The GMP impact and risk assessment, built into the release notes
- Functional test evidence for every change with a high GMP impact
- A signed release approval and fit-for-release conclusion
- An open-issues list: known GMP-impacting defects and recorded exceptions

Between releases

We notify you within five business days of a confirmed defect in GMP-critical functionality that affects a version you run.

Who does what

AZUMUTA PROVIDES	YOU PROVIDE
Controlled, documented development of the software	Infrastructure, installation and the running environment
GMP documentation: release notes, validation package, capability statement, installation guide and IQ checklist, GAMP 5 mapping	Backup and disaster recovery
Functional and regression testing from our automated builds	First-line support for your users
Change and defect notification	Your own validation: IQ, and PQ or UAT against your user requirements
Support to your IT during installation and qualification	Accountability for data integrity and validated state, as the regulated company

DOCUMENT 2

21 CFR Part 11 and EU GMP Annex 11 capability overview

What the platform does for each area of 21 CFR Part 11 and EU GMP Annex 11.

Audit trail

Part 11 §11.10(e) · Annex 11 §9

Every action that can be executed in the platform is registered in the audit trail, with who did it and when. Entries can't be changed or removed, not even by an admin.

Electronic signatures

Part 11 §11.50, 11.70, 11.100, 11.200 · Annex 11 §14

Sign-offs, revision approvals and signature or double-check steps are each tied to a named person, a timestamp and the record they sign. People confirm who they are with their own password or SSO, and authors can be blocked from approving their own work.

Access and authority

Part 11 §11.10(d), (g) · Annex 11 §12

Every action belongs to one personal account. There are no shared logins. You set rights at user group level, and SSO (OIDC or SAML), SCIM provisioning and two-factor authentication are supported.

Record integrity and retention

Part 11 §11.10(a), (c) · Annex 11 §4, 7, 17

Every product order and digital checklist is stored in the database, and every revision is kept as a full copy. A finished digital checklist only changes through a controlled rework step that needs the right permissions. You decide how long the data is retained.

Copies for inspection

Part 11 §11.10(b) · Annex 11 §8

Records export as PDF, DOCX, XLSX, CSV or JSON. Each approved revision gets its PDF at the moment of approval, and that PDF stays with it. A REST API gives read access.

Time and sequence

Part 11 §11.10(e), (f)

Audit trail timestamps come from the server. Work done offline keeps both the device time and the time it reached the server. Status changes, step order and required checks are enforced.

The full capability statement covers each area in detail. Ask your Azumuta contact for it.

DOCUMENT 3

How validation works with Azumuta

You know how to validate. We know our product. Below, deliverable by deliverable, is what comes from us and what stays with you, following a GAMP 5 approach.

DELIVERABLE	WHO	WHAT IT INVOLVES
Validation plan	You	Your template and approach
User requirements (URS)	You	Your process, your intended use
Supplier assessment	Both	Supplier Qualification Dossier, Quality Agreement, audit of how we develop and release
Functional and design specifications	Azumuta	Kept per requirement in our development records, linked from the release notes
Installation Qualification (IQ)	You	Our installation guide and IQ checklist
Supplier testing	Azumuta	Functional and regression testing from our builds, test evidence for every change with a high GMP impact
PQ or UAT	You	Against your URS, with your procedures and templates in Azumuta
Traceability	Both	Release notes link each change to its requirement and test, you trace to your URS
Validation summary report	You	Our signed release approval feeds your report
Change control after go-live	Both	Release notes show the GMP impact of each change, so you know which ones to assess

Starting small? You can validate one use case at one production site first, then roll out further later on. The templates from your first site are there as a starting point for the next ones, but you don't have to use them.

DOCUMENT 4

Release and change summary

Every change to a validated system means revalidation. So you decide which releases to take, and when. Each release lists what changed and how it affects GMP.

How releases reach you

One product and one codebase for every customer. You download the installation package of the version you choose and install it yourself, or with help from our professional services team.

When something goes wrong

If an issue comes up, we fix it within five business days. The fix follows the same review, checks and approval as every other change.

What comes with every release

A full changelog with the GMP impact of each change, the risk assessment, test evidence for high-impact changes, a signed approval and the open-issues list.

Skipping releases

You decide which releases to install and which to skip. When you catch up later, for example because a new site joins, that can mean a minor revalidation of the changes in between. You get the documentation of every release you skipped.

DOCUMENT 5

Hosting, security and continuity

GMP customers run Azumuta on their own infrastructure, inside their own security and GMP hosting rules.

On your own servers

A containerised installation on your own servers. You can run GMP and non-GMP instances side by side, so new features reach non-GMP work first. That combination is an option, not a requirement.

Keeps working offline

In the browser or the app, operators keep working when the network drops. Events are queued on the device and synced without duplicates once the connection is back, with device and server time both kept.

Ready for your business continuity plan

If your infrastructure or network fails, you still have an offline copy of every instruction and execution, so your business continuity plan always has a current version to fall back on.

Control your access

Personal accounts, SSO through OpenID Connect or SAML, SCIM provisioning, optional two-factor authentication, per-device API keys and session timeouts.

Data protection

- Files stored as private objects, never publicly readable, with every download checked on the server
- Uploads verified against a SHA-256 checksum
- Workspaces isolated from each other, with automated checks on data scope in the code

Shared responsibility on-premise

AZUMUTA	YOU
Application-level controls: audit trail, rights, versioning, private file access	Servers, network isolation and database hardening
Installation package and guide, support during installation	Backup, disaster recovery and restore testing
Security policies, published in our Trust Center	Clock synchronisation for servers and devices