

Software for biotech instrumentation: **GMP**, validation & best practices.

A practical guide for instrument manufacturers selling into GMP-regulated laboratories - covering regulations, manufacturer's responsibilities, and the best practices that make compliance achievable.

Executive summary.

Software is a crucial part of biotech instrumentation as not only does it handle data capture and analysis, but also user management and data traceability. It is also where users will spend the majority of their time interacting with the instrument.

For instruments sold at scale, especially into Good Manufacturing Practice (GMP) certified labs, software must also ensure data integrity, traceability, and compliance with global regulations. Failure to meet these standards creates barriers to purchase for GMP labs that would otherwise be potential customers.

This white paper has been developed by experts at Firefinch Software to help manufacturers develop their instrumentation to comply with GMP regulations. It covers the key regulations and standards, responsibilities of the manufacturer, as well as best practice in software development, cybersecurity and stage-gated development.

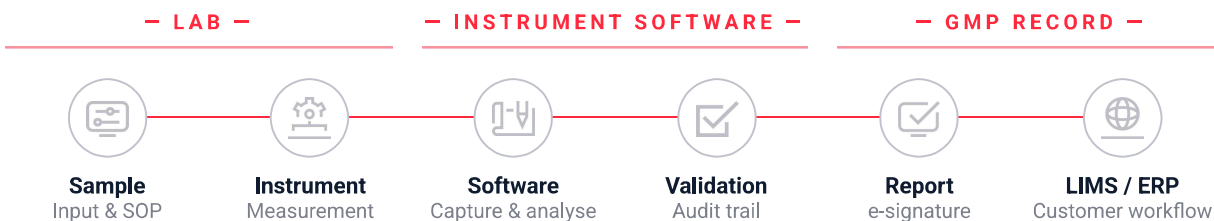


FIGURE 01 A biotech instrumentation process — from sample to validated record. Every transition is an opportunity for the software to either support compliance, or quietly undermine it.

Instrumentation companies are often caught off guard by the software side of GMP. A buyer who needs audit trails, electronic signatures and ALCOA++ data integrity will walk past a brilliant instrument whose software can't deliver these capabilities.

— RUAÍDHRI PRIMROSE, DIRECTOR, FIREFINCH SOFTWARE

CONTENTS

What's inside

01 Executive summary	02
02 Introduction	03
Who are Firefinch?	03
The importance of software in biotech instrumentation	04
What are the risks if you don't get this right?	05
03 Key regulations and standards	06
04 Core functionality and data management for GMP	07
Good Documentation Practice (GDocP)	08
05 Responsibilities as the instrument manufacturer	11
Quality management system	11
Validation parameters	11
Instrument qualification – DQ, IQ, OQ, PQ	12
Failure Mode and Effects Analysis	13
Cybersecurity	14
AI and ML	15
06 Best practice in software development	16
User-centric design	16
Software localisations	16
Stage-gated development	17
When to hire and when to outsource	19
07 Conclusion	20

02

Introduction.

Who are Firefinch?

Firefinch Software partners with life science companies to develop custom software that is scientifically grounded, regulatory-ready, and built to scale. Their expert-led team brings together domain knowledge, compliance expertise, and strategic insight to help organisations bring the right product to market.

The company was founded in 2017 by a team of senior software developers that built software for some of Agilent's flagship biotech instrumentation.

Now a team of nearly 30 people, based in Edinburgh, Firefinch regularly serves biotech and medtech instrumentation clients and has deep expertise across photonics, machine learning, microbiology, mass spectrometry, biomanufacturing and medical devices.

The importance of software in biotech instrumentation

Biotech instrumentation is a broad term that includes any instrument that measures or produces a biological product. This might include DNA analysers, whole cell analysers, bioreactors, chromatography instruments, spectrophotometers, image analysis tools and more. Instrument control software performs a variety of roles including data capture, data analysis, data management, robotics control, process control and system integration.

Instrument software is often a critical part of how a measurement is taken and reported to the user. The user may also want to interact with the readout by using the software and may want to produce reports. How this software looks and feels is important to how the instrument is viewed and sold.

If an instrument manufacturer wants to sell at any scale, then the software will also need to be able to integrate into labs that have higher auditing needs than a simple, unvalidated readout. This might include:

- keeping track of instrument validation and auditing
- Standard operating procedures and any deviations from the assay
- Which consumables were used and under what conditions
- Validation data of the biological product (if there is one)
- Data processing and auditing
- User management – who produced what data and who viewed what data

All of this will be built into the software to help manufacturers provide a validated product to their customers that can be scaled.

The ultimate aim is to provide an instrument that is high quality and reliable for GMP customers. This paper will cover the development of software for instrumentation wishing to sell into Good Manufacturing Practice (GMP) or Good Laboratory Practice (GLP) certified labs. We will cover product development life cycles, what teams need to consider as they develop instrumentation and how to ensure instruments can easily integrate into customers' workflows.

What are the risks if you don't get this right?

The development of GMP standards has historically been driven by high profile scandals involving poor quality manufacture of medicines and food. The regulations are now seen as a proactive way to ensure quality, rather than a reactive response to issues. There can be large penalties if non-compliance is detected or if adequate record keeping is not maintained.

Aside from the risk of fraud, there are also strong commercial advantages to making instrumentation capable of GxP compliance. Imagine a pharma company is considering buying a new spectrophotometer to analyse DNA purity and quantity. Instrument A might be cheaper than the market leader and have beautiful looking software, but if Instrument B comes with all the validation paperwork, built in validation processes and integrations to the rest of the company's workflow, then the pharma company is unlikely to take a risk on Instrument A. No company wants to be audited and realise that they don't have all the paperwork for their regulated product, so Instrument A is not worth the risk.

GxP

Good Practice guidelines and regulations exist to ensure that food, medical devices, drugs and other life science products are safe, effective and usable. They are backed by the European Medicines Agency (EMA), the World Health Organization (WHO), the U.S. Food and Drug Administration (FDA), Medicines and Healthcare Products Regulatory Agency (MHRA) and the International Organization for Standardization (ISO).

- | | |
|--------------|---|
| GMP | Good Manufacturing Practice is a minimum standard that manufacturers (including food, medical devices and pharmaceuticals) must meet in their production processes. Products must be of a consistent high quality, be appropriate for their intended use and meet the requirements of the marketing authorisation or product specification. |
| CGMP | Current Good Manufacturing Practice emphasises the use of continuous improvement and adaptation to modern practices to comply with GMP requirements. |
| GLP | Good laboratory practice is the set of recognised rules governing the conduct of non-clinical safety studies. They ensure the quality, integrity and reliability of study data. |
| GDocP | Good Documentation Practice is a systematic procedure of preparing, reviewing, approving, issuing, recording, storing and archiving of documentation. |
| GCP | Good Clinical Practice is the agreed international standard for conducting clinical research. |

Key regulations and standards.

The use of software in GMP environment is subject to two crucial pieces of regulation: **FDA 21 CFR Part 11** regulation applying to products to be sold in the USA; and **EudraLex Volume 4 Annex 11** requirements on computerised systems used in GMP manufacturing of medicinal products for human and veterinary use within the EU and adopted across the EEA. Both documents define the requirements on the software, and software providers, which include:

- Record generation and protection
- Security control
- Operational control
- Data control and audit trails
- User authentication
- Electronic signatures

EudraLex Annex 11 contains more detailed requirements than 21 CFR Part 11, which applies specifically to electronic records and signatures that are created, modified, or transmitted under FDA regulations and has a scope primarily related to the records themselves rather than the how the system was produced which creates them, whereas Annex 11 defines additional requirements on the entire software lifecycle, risk management, quality management systems, and validation of the software suppliers.

There are also several international standards relating to instrumentation

ISO 9001

For quality management systems.

ISO 14001

Environmental Management System.

GAMP 5

Good automated manufacturing practice for pharma and life sciences.

ISO 31000

Risk Management.

ICH Q2(R2) guidelines

Validation of analytical procedures.

USP 1058

Analytical Instrument Qualification.

Medical device regulations also require alignment to international standards. See our tech note on medical devices and our blog articles for more detail on how to develop software under this framework.

Core functionality and data management for GMP.

To sell instrumentation into a GMP environment it is important to understand what the requirements of GMP involve. There are requirements in staff knowledge and responsibility, product specifications, process documentation and control, procedures and guidelines for the processes and maintenance and calibration of equipment.

GMP premises will be audited on a regular basis to ensure compliance to GMP regulations and performance will be monitored to detect any drift in quality.

The 5 P's of Good Manufacturing Practices

 People Clear roles and responsibilities	 Products Specifications at each production phase	 Processes Clearly and consistently documented	 Procedures Guidance for critical processes	 Premises Continuous maintenance and calibration
--	---	--	---	--

FIGURE 02 The 5 P's of GMP — people, products, processes, procedures and premises.

When describing the core functionality of an instrument it is important to be absolutely clear and not to be tempted to make marketing claims that cannot easily be backed up with robust data. Clarity is needed on the limits of what the instrument does and under which conditions. For example, a claim such as **“My instrument can quantify protein”** is vague and would very quickly lead to further questions from a user such as:

- What is the limit of detection?
- Does it measure all protein or specific proteins using markers?
- What temperatures does it work at?
- How robust are results between instruments?
- What reagents can I use?
- How accurate is it?
- How repeatable is it?

To answer any of these questions manufacturers need to have proof and a validation method for each claim and under each set of conditions. A more sensible claim might therefore be **“My instrument can measure haemoglobin within a range of 46 pM to 2 µM under standard operating procedures”**. A defined SOP for haemoglobin detection would be provided, outlining exactly which reagents to use and under what conditions.

Data should also be collected to prove that users follow the SOP as intended. For example, if an instrument doesn't have a sensor and reporting process for monitoring temperature fluctuations, then there will not be an audit trail to prove that users followed the SOP with regards to the temperature range. Developing the software that takes an electronic signal and produces a readout for a user (cell number, microscope image, DNA sequence) is therefore only part of the software for an instrument. Not taking into account developing the traceability, validations and documentation to support the readout will rule out sales to GMP labs, which are a large portion of the market.

The data produced to provide that traceability and evidence that an instrument conforms to GMP (or GLP) will be managed by GDocP.

GDocP

Designing software to comply with GDocP requires an understanding of GMP and what the compliance requirements are.

For an instrument manufacturer it is good to be able to say to customers that data integrity and data traceability are high priority in the software and a large part of GMP manufacturing relates to data storage and traceability. This will be particularly pertinent if the instrument performs data transformation or produces reports. The extent to which there is traceability around supporting data integrity becomes good documentation practice.

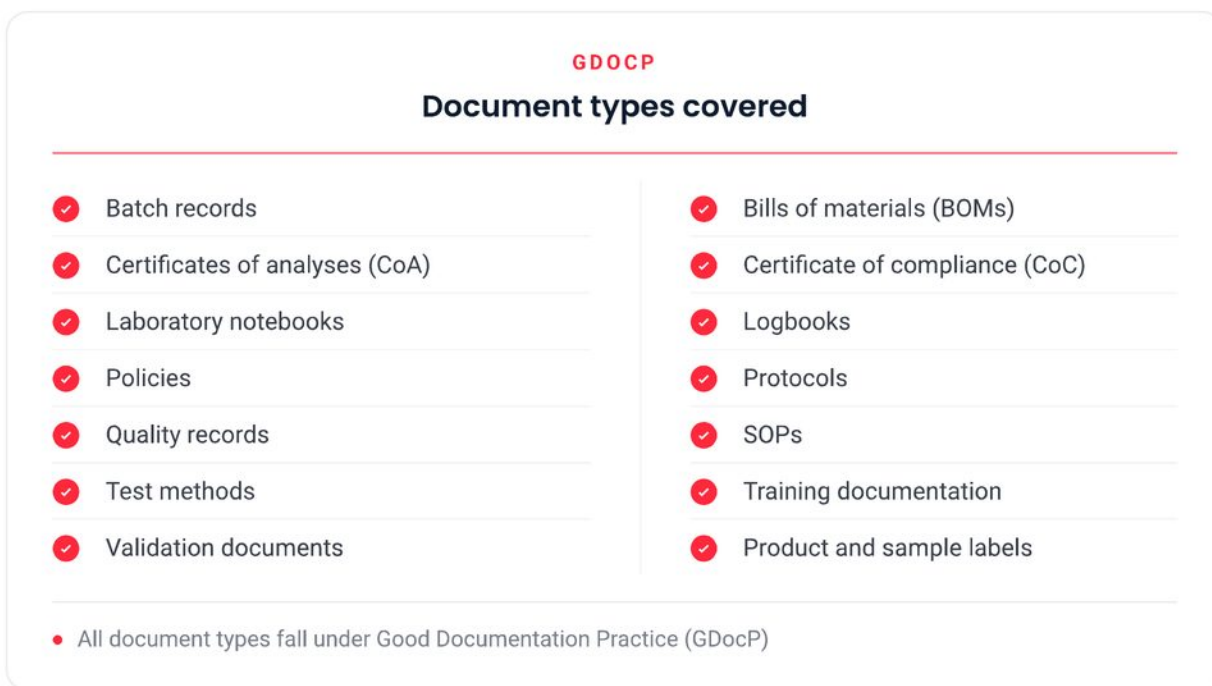


FIGURE 03 The document types GDocP covers — from batch records to training documentation.

Electronic signatures

With paper documentation, data are attributed to users through physical signatures – the person that ran a data analysis would sign and date identifying the method and reagents used. Electronic records need to be similarly signed and dated, which forms part of 21 CFR Part 11 compliance, covering how electronic signatures are implemented. The records need to be enforceable as equivalent to a paper signature in a court of law, so the software needs to be built in such a way that it is impossible for one user to sign as another user. Building an instrument with robust user management – security, audit and electronic signatures – will therefore help customers stay compliant.

Data storage and access

Another part of GDocP is validation of data storage and integrity. Instrument manufacturers will need to ensure that data has been stored securely and any attempts to tamper with stored data would be detected. There should therefore be a record of who has logged in and out and, when and what changes (if any) have been made.

File formats and customer workflows

Providing data in a standard format, rather than a proprietary format will make it easier to prove compliance as well as making data management easier for customers. A proprietary file format will also increase risk for customers if the manufacturer goes out of business or the software is no longer supported. A large barrier for entry for customers will be whether the instrument is compliant with internal systems such as LIMs, ERP, and analytics platforms, so this should be a high priority when designing instrument software.

ALCOA for data integrity

ALCOA is a core principle of GDocP. The acronym originally stood for **A**ttributable, **L**egible, **C**ontemporaneous, **O**riginal, and **A**ccurate and was used as a set of data integrity principles in the pharmaceutical and other industries. The term has more recently been updated (ALCOA+ and ALCOA++) to include **C**omplete, **C**onsistent, **E**nduring, **A**vailable, **T**raceable to account more for automation, cloud-based environments and electronic records.

COMMON MISTAKES IN GDOCP

Auditable requirements versus implementation

We often see companies get bogged down in the details of requirements and overcomplicate the standards.

Thinking that a piece of software can be compliant

An installation of the software cannot be compliant in itself without taking into account the environment and the process and procedures around it. A better way to describe compliance is to say that if the software is installed correctly and used for its intended purpose then it should pass audit for that purpose.

Not thinking about reporting early enough

The report an instrument produces is the real product. During instrument development, reporting is often thought about once the engineering parts are complete but should be part of the documentation design from the beginning.

Responsibilities as the instrument manufacturer.

It is important to understand where responsibility lies between the manufacturer of biotech instrumentation versus the clients that manufacture regulated products such as pharmaceuticals or food or provide regulated testing services to clients. Instrument manufacturers will be expected to have a quality management system in place, including standard operating procedures (SOPs). The manufacturer will also need to be able to prove, or provide the capabilities for customers to prove, that the instrument is validated across its lifecycle – from design to performance in situ.

Quality management system

In a CGMP environment, there will very likely be a QMS in place to ensure that all the documentation is in place for ISO 9001 compliance. The QMS should document everything needed to run a process including SOPs. If a user doesn't follow the written process, then there has been a deviation. The deviation should then be assessed as minor or major – major meaning that the product has been affected. Risk management techniques must therefore be used to identify where deviations are likely and to influence the design to reduce the risk of them.

The geographical contexts (localisations) where the instrument will be used should be considered within the QMS and SOPs and user interfaces may need to be written in local languages to avoid misunderstandings that can lead to non-compliance. There are many QMS tools on the market that help ensure documentation is well organised.

Validation parameters

Before market release of a new instrument, the manufacturer will usually want to produce evidence of the validation of their instrument (and their assay). This will enable them to make claims on parameters such as:

- **Accuracy:** How close the measurement is to the right answer.
- **Sensitivity:** How dilute a sample can be detected.
- **Linearity:** How well scaled measurements are over a concentration range.
- **Precision / Repeatability:** What variation is there when the same sample is measured repeatedly.
- **Intermediate precision:** Variation when the same sample is measured on different days by different people on different instruments.
- **Reproducibility:** Variation when a measurement is repeated in different labs on different equipment.
- **Robustness:** How sensitive the method is to deliberate variations in method parameters.
- **Working range:** The range within which measurements are valid.

For an instrument manufacturer, perhaps the most difficult parameters are the interplay between precision, repeatability, reproducibility and robustness. Producing a hundred instruments every month, with 10 different batches of consumable and 50 different batches of reagent, which will be shipped around the world, produces a lot of variation that could affect the performance of the product.

The best way to tackle this level of variability is to consider all variables from early in the development process – and to measure their impact as early as possible. The deeper the understanding of this complex interplay, the better knowledge a company will have of the sensitivities of the system and how these can be detected and remedied. It can feel too early to measure these parameters, but the knowledge is useful to have as early as practicable to understand the performance specifications of the instrument.

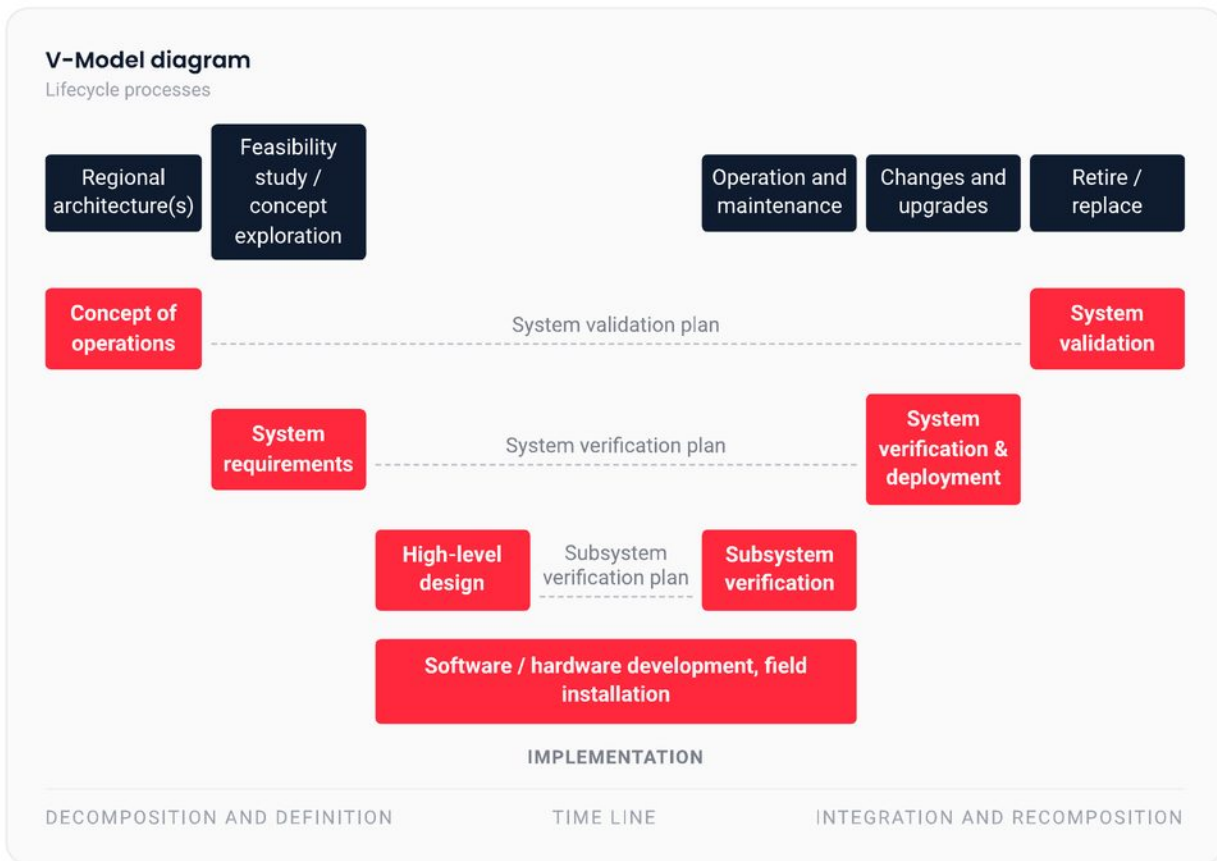


FIGURE 04 Image modified from [The V-Process Demystified: Phases and Importance | WiredWhite](#).

Instrument qualification – DQ, IQ, OQ, PQ

There are a few qualifications that an instrument manufacturer will need to enable to ensure correct installation and operation of the instrument by the users.

Some of these qualifications, such as DQ, are burdens on the manufacturer and some, such as PQ, are a burden for the user. Qualifications such as OQ and PQ will need to be repeated regularly to prove that the instrument still works as expected, and some (IQ, OQ and PQ) will need to be performed each time the instrument is moved, or a part has been changed. The instrument manufacturer should make it as easy as possible for the buyer to qualify their instrument (including software). For those that will be performed regularly, there will usually be a software prompt to remind users to do this.

Instrument qualifications

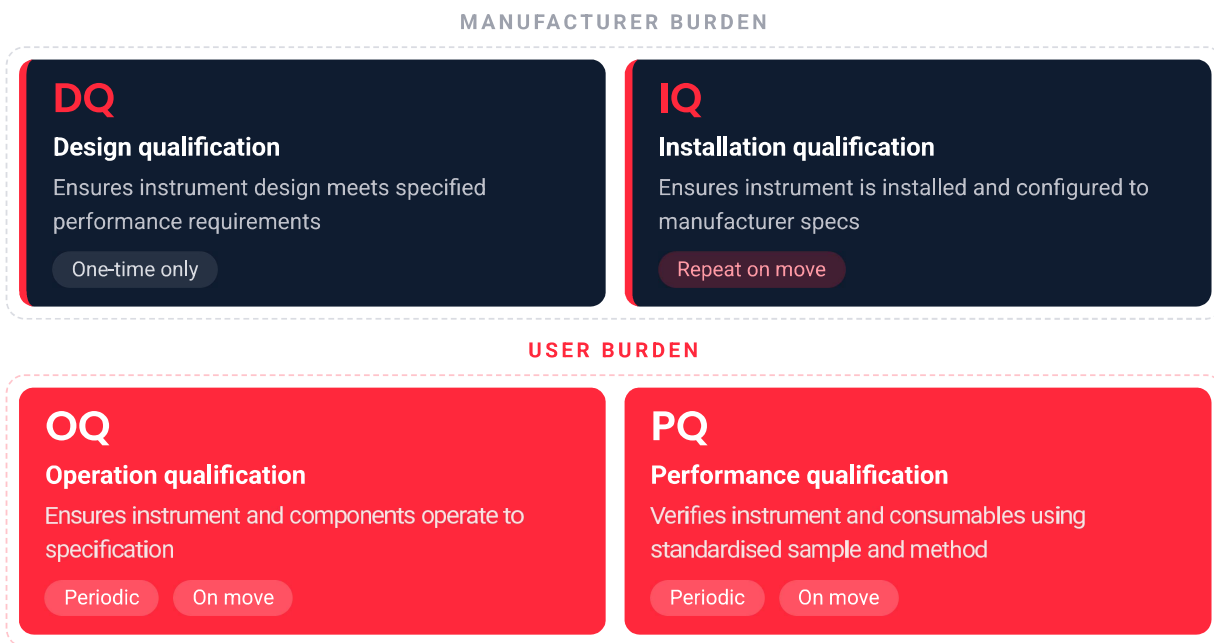


FIGURE 05 The four instrument qualifications — manufacturer burden (DQ, IQ) and user burden (OQ, PQ).

Failure Mode and Effects Analysis

FMEA is part of product risk management and is important to identify product design risks. FMEA should be set up as a systematic, step-by-step process to identify potential failures in design, manufacturing and process. Risks can then be prioritised for mitigation.

An example failure mode that could arise might be the blank and sample being input in the wrong tube in the instrument. A risk analysis would look at whether there is a critical effect on the instrument or results. A mitigation to this failure mode might be displaying a warning that the blank does not seem to be blank (increase detectability) and allowing the user to re-label the sample and blank after input into the instrument. Using colour coding might avoid the mistake (reduce frequency).

Cybersecurity

Instrument software is an attractive target for attackers, particularly when used in environments such as GMP facilities where downtime is expensive and high-value IP is being processed. GMP lab managers will need to assess that the instrumentation they purchase does not introduce cybersecurity risks into their business.

There are several areas that need to be evaluated, with common areas of concern being:

- 01 Connectivity** – Often in legacy systems connections from instruments to other systems such as LIMS and ELNs are not properly authenticated or encrypted.
- 02 Patching and support** – A plan must be in place to ensure systems remain on in-support versions of software from vendors, including their operating system. If vulnerabilities are disclosed in third party software, a plan must be in place to address these.
- 03 Account security and audit trails** – The use of shared accounts and a lack of role-based permissions is common, making audit trails and access controls effectively meaningless.

Cybersecurity needs to be built into a QMS across the product development lifecycle and not treated as a late-stage concern. This often includes aligning with cybersecurity standards such as ISO/IEC 27001 and IEC 62443.

AI and ML

Many instrument manufacturers are making use of advanced algorithms such as machine learning (ML) to interpret data. These algorithms will introduce additional risks that will need to be addressed in the QMS. Some of the additional risks that might be encountered arise from:

- **Training data quality and bias.** A model is only as reliable as the data it was trained on. Underrepresented sample types, mislabelled data, or training sets collected on different instrument versions can produce models that silently perform poorly in production.
- **Adversarial inputs.** Where models are updated from live data, an attacker can introduce examples designed to degrade performance or induce specific errors.
- **Model drift.** The real-world distribution of results shifts over time, for example due to new reagent lots or changed operating environments. A model that was accurate at release can degrade without anyone noticing unless drift detection is built in.
- **Explainability.** Many modern ML models are effectively black boxes. Under audit, a customer may be required to explain why the instrument produced a particular result, and a model that cannot be interrogated becomes a liability for them.
- **Reproducibility.** In general, there is a regulatory and compliance need that the same input should produce the same output. Non-determinism and continuous learning can break this assumption.

Complicated data models make validation more difficult, and the onus will be on the users to explain how the model works should they get audited. Building explainability and risk mitigation of AI/ML models into the documentation will therefore be important to customers working in regulated environments.

Best practice in software development.

User centric design

A term often used in user centric design is the pit of success: it should be easy to succeed and difficult to fail in well-designed software. Good design means that the product has been designed in such a way that a user is constantly guided into following the correct procedure. Surprise is considered to be bad in design terms – it should always be obvious what is happening and why.

Due to the variability of users over the product development life cycle, many manufacturers develop two software packages in parallel – one for internal use and testing and one for full validation. The final, validated instrument will be streamlined for a specified use. There may also be a method development view of the software, which has more functionality than the standard SOP view and stage-gated approval as the new method becomes a validated method that can be run using an SOP.

Software localisations

Many instrument manufacturers intend to sell their instrument globally. Knowing that the software will be translated for local contexts is important to understand when completing the QMS and the user interface. The risks of not getting this right can lead to variability in regional compliance as users in some geographies may not understand SOPs and instrument operation as they should when not presented in their native language.

Planning for translation of the user interface, training and SOPs from the start will reduce these risks. On the software side, building in an addon that can allow translation of user interface screens is a cheap and effective way of ensuring translations can be made as required. The addons allow the interface to be exported in a standardised format (csv, xls, json or xliiff) to enable multi-lingual menus to be created.

Menus should be tested in all languages to ensure special characters can be seen and text boxes are large enough for all localisations. This is important as some fonts will not allow for some characters, such as Chinese ones.

For manufacturers selling into the European Union, language requirements are checked on a case-by-case basis, but standard practice will be to include 24 EU languages.

Stage gated development

A common mistake some manufacturers make is thinking that testing is not needed until later stages of development. They will start with an early prototype, plan a second version then plan validation for the final version. In reality, testing, verification and risk assessment needs to be conducted constantly so that manufacturers can build a robust understanding of the system and its sensitivities. If weaknesses are built into the system, they can be very difficult to correct.

It is a good idea to follow a stage-gated development process to ensure that essential criteria, such as value generation and risk management, have been met before moving on to the next stage of development. There are a few models available that can be followed. Here, we reference the stage gate model, a version of which is used by many large companies, such as Agilent and Thermo Fisher Scientific. Each stage of development is concluded with a go/kill and resource-allocation for the next stage and allows senior leaders to assess the project's business value and readiness.

Stage Gate Development Process

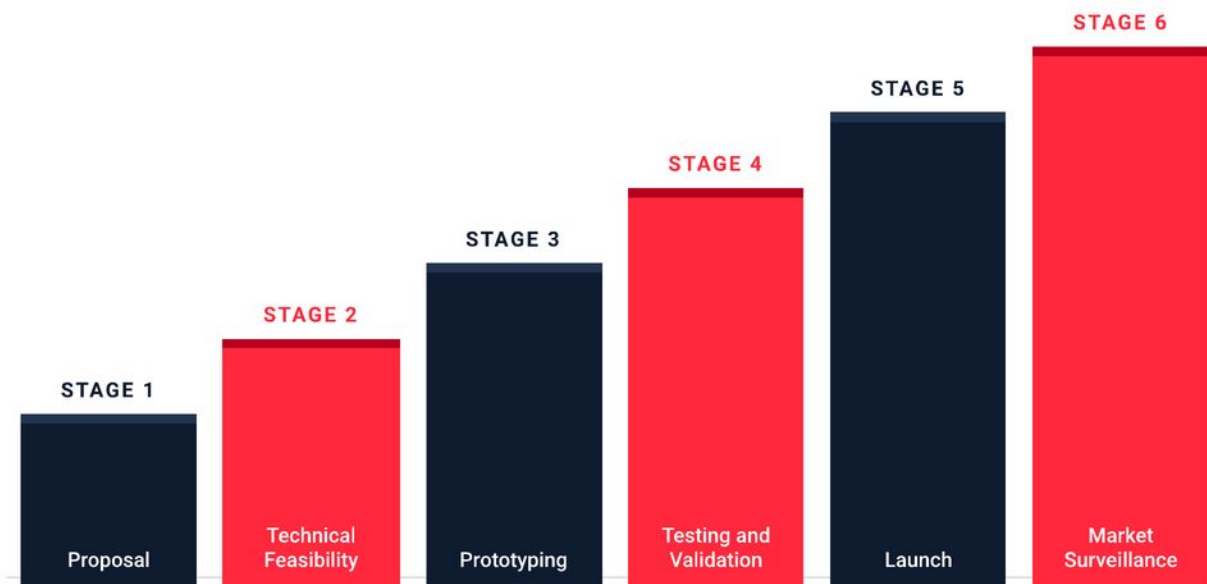


FIGURE 06 Stage gate model — a version of which is used by many large companies, such as Agilent and Thermo Fisher Scientific.

The stage gate model

DISCOVERY

Discovery and Ideation

Upstream activities designed to uncover opportunities and generate ideas. Inputs can come from customers, internal R&D, suppliers, and strategic initiatives. The aim is to populate the front end with strategically aligned high-potential ideas.

STAGE 2

Technical Feasibility

A more detailed and evidence-based investigation. This stage typically includes primary market research, competitor analysis (and parameters to measure against), voice of the customer studies, technical feasibility studies, value proposition clarification, financial evaluation, a regulatory plan and risk assessment. The key output is a robust business case, specifying the product definition, market positioning, financials, and a plan for further development.

STAGE 4

Testing and Validation

Rigorous validation of the product, how it will be marketed, and the production or service delivery system. This stage typically includes beta tests, user pilots, field trials, extended lab testing, and trial production runs. The goal is to confirm that the product performs as promised, the market will accept it, and operations can deliver reliably at scale.

STAGE 6

Post Market Surveillance

Monitor performance, resolve issues, implement CAPA (corrective and preventive action) and complaint handling, and drive product and process improvements.

STAGE 1

Proposal

A quick, preliminary assessment of the idea. Teams conduct initial market and technical scoping using desk-based research and analysis. The outcome is a clearly defined proposal, with a first view of business value and feasibility.

STAGE 3

Prototyping

Detailed design and development of the product and supporting operations or production processes. Activities include engineering design, optimisation, simulations, prototyping, and process design. The main deliverable is a fully functioning prototype ready for customer and field testing.

STAGE 5

Launch

Full commercialisation and increasing manufacturing and operations; execution of the launch, sales, and marketing plans; and roll-out to target markets.

In a software context, the code will be managed at each stage through an appropriate software development lifecycle and this should be developed alongside the whole product as part of the stage gate model.

It is important to ensure there are very clear criteria for when to move through a stage gate. This should be in the form of evidence required and if there is some evidence missing then the gate should not be passed.

When to hire and when to outsource

There should never be one person in a company that oversees ensuring compliance – rather it should be woven into everything the company does. There are, however, a few key roles that need to be on top of the regulations and how the instrument is going to meet them. Some regulations require a named responsible person. Suppliers also need to be qualified as fit for purpose.

Many start-ups and SMEs will hire external resource during the development of a new device. It is common to work with product design agencies and specialised software developers to enable quicker development and compliance.

Best practice is to engage early to build relationships and confidence in service providers.

PRODUCT OWNER

It is common to have a product owner that manages development of the product and ensures stakeholder views are translated into actionable updates for the product development team.

QUALITY ASSURANCE LEAD

Ensures quality product including ensuring the cold chain is validated for shipments, that drop testing has been completed, that admission testing has been completed etc. The QA lead will lead continuous process improvement and monitor customer feedback.

PRODUCT DEVELOPMENT TEAM

Ensuring product performance, performing the validation, designing the validation studies, processing the results and reporting back to stakeholders.

CYBERSECURITY TESTER

Usually external experts who perform vulnerability assessments and penetration tests.

CEO / CSO / CTO

The senior management team need to be fully aware of how the instrument will meet compliance and what this entails.

Conclusion.

If an instrument manufacturer wants to access the biotech market at any scale, they cannot ignore GMP standards. Providing software that can support users to remain compliant and make the auditing process easier is not just good practice – it makes good business sense.

Following a rigorous, stage-gated development process supports data quality and compliance at each stage of development, ensuring that evidence can be provided for every claim made of the technology.

There is much to consider when developing an instrument to GMP standards. Engaging experts early in development will prevent costly mistakes and delays, getting a compliant product to market, faster.



Firefinch Software

SOFTWARE DEVELOPMENT
SUPPORT



Lorit Consultancy

CYBERSECURITY SUPPORT



Transcom Global

TRANSLATION SUPPORT

To read more about how the Firefinch team support biotech companies with GMP development, take a look at our case studies.

[Read our case studies →](#)

CONTACT

contact@firefinch.io
firefinch.io