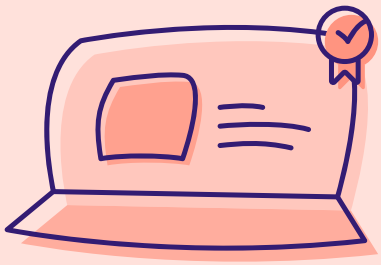
Qualio



Complete guide to computerized system compliance in 2023

With input and expert advice from Sion Wyn
GAMP SIG expert, GAMP 5 editor,
FDA 21 CFR Part 11 advisor

Table of Contents

As a provider of electronic quality management software to regulated life science companies, it's crucial that Qualio remains in lockstep with the latest regulatory demands and expectations.

As I speak to prospective Qualio customers, it's clear that there's still plenty of uncertainty, and unnecessary fear, in the life science world around one area in particular: computerized system compliance.

What does modern CSV really demand for electronic quality management system adoption?

What will my auditor expect to see when I show them the eQMS software we've been using?

Do we still need IQs, OQs and PQs? These are common and recurring questions.

We've assembled this guide, with the help of computerized system compliance expert Sion Wyn, to answer these questions for you.

A new chapter of computerized system assurance, driven by critical thinking and agile, risk-based digital quality, is opening to replace the bloated, burdensome and paper-heavy legacy of computerized system validation. Use this guide to bring your business into line with the latest FDA, EU and ISPE expectations and drive a confident, compliant adoption of computerized tools.

Kelly Stanton
Director of Quality, Qualio

The paradigm shift: CSV to CSA

The primary recent development in the world of computerized system compliance is the shift from computerized system validation to computerized system assurance.

What's driving the shift? And what does it entail?

In a nutshell, the FDA *wants* life science businesses to invest in computerized systems that digitize, automate and accelerate quality and manufacturing processes. These systems, after all, slice the risk of human error. They free up manual admin time for continuous improvement and quality assurance work. And they contribute to faster, safer delivery of life-saving products to patients.

But the requirements of computerized system validation, outlined in the FDA's 1997 *General Principles of Software Validation*, were seen to discourage this adoption of digital tools by presenting an image of unnecessary burden to regulated companies. Written when they were, CSV guidance had to be stretched to match the 21st-century world of CRMs, LIMs and eQMS platforms.

In the absence of updated guidance, many businesses fell back on conservative, time-consuming validation processes for fear of being non-compliant.

Some businesses gave up altogether. Rather than going through what was perceived as a time-heavy, expensive and laborious validation process, they chose to stick with basic quality management tools like paper and

spreadsheets. After all, they require no rigorous setup and can be applied instantly. By our count, around 38% of life science companies continue to use this ingrained manual approach in 2022, particularly start-up and scale-up businesses.

The consequences of this hesitation to digitize can be profound. Companies reliant on legacy quality tools continue to spend inordinate amounts of time on paper-pushing and battling leaky, uncontrolled information flows. Our quality trends survey revealed that over half of life science quality professionals spend a quarter of their working day *just* populating spreadsheets, producing reports or searching for information.

This saps time from the real quality work of continuously improving product and patient safety. And it blocks the industry best practice outlined in GAMP guidance from the FDA and ISPE.

> ***Where there aren't the tools and systems in place, there aren't enough resources or energy to put into quality improvement. 80% of the effort should be there, but currently it's where only 20% of time is spent. This means we're not focusing on the bigger picture, which is patient safety.***
>
> **— Sion Wyn**

The evolution from CSV to CSA aims to make the adoption of compliant computerized system tools simpler, more streamlined and more straightforward. In the FDA's words, the 'least burdensome approach' is to be followed – as long as the proper care is taken to safeguard the integrity and quality of the products you make.

Instead of producing lots of documents to *validate* a digital system and show to auditors – who, incidentally, are only interested if there's a direct high risk to patient safety at play – regulated companies should instead adopt an agile and risk-based *assurance* approach to the tools they adopt, trusting system vendors to perform their own testing activities and supplementing sensibly for high-risk areas as required.

The logic is clear:

Faster, simpler computerized system onboarding

Higher adoption

A more digitized life science world with modern tools and techniques

Computerized system assurance focuses on:

Critical thinking and risk-based adoption of computerized tools

Jettisoning of unnecessary legacy validation documents, like IQs, OQs and PQs

Eliminating fear of regulatory inflexibility as a blocker to the adoption of new technology

A return to the original 'spirit' of GAMP:

- Proving your computerized system is fit for intended use
- Ensuring your computerized system meets the basic baseline of compliance
- Managing any residual risk to patients and to the quality of the final medicinal product

Above all, it's important to note that CSA isn't 'new' in the strictest sense of the word. On the contrary, it's designed to remove the perceived barriers standing between life science companies and the innovative, agile approach to computerized system adoption already outlined in GAMP 5 and its associated Good Practice Guides.

To that end, the emphasis for modern computerized system compliance falls on cultural change within regulated businesses, rather than any dramatic overhaul from the regulators themselves.

The FDA's 2022 CSA guidelines

The FDA unveiled its draft guidance, "Computer Software Assurance for Production and Quality System Software", in September 2022.

The draft is open for comments from the public until mid-November, and aims to formalize and document the new world order of computerized system assurance.

It's a useful draft to explore for an early feel of how the FDA envisions a modern and optimal CSA approach. The draft offers a definition of computerized system assurance, and some assurance and testing methods and objectives. The document particularly focuses on medical device organizations, and how computerized system assurance can support compliance with the Part 820 Quality System Regulation.

Key takeaways include:

Clear definition

The FDA confirms the general principles of CSA that we've already explored, defining it as:

> ***...a risk-based approach for establishing and maintaining confidence that software is fit for its intended use. This approach considers the risk of compromised safety and/or quality of the device... to determine the level of assurance effort and activities appropriate to establish confidence in the software.***
>
> ***Because the computer software assurance effort is risk-based, it follows a least-burdensome approach, where the burden of validation is no more than necessary to address the risk. Such an approach supports the efficient use of resources, in turn promoting product quality.***

Step-by-step risk framework

Regulated companies completing a CSA process should:

1. Identify the intended use of the software

- Is it a direct part of the production or quality system, or a supporting element?
- Are there multiple uses arising from multiple features, functions or operations?

2. Determine the risk-based approach

- Based on the intended use, what is the risk profile of the software and its potential impact on product and patient safety?

3. Determine appropriate assurance activity

- How much objective evidence is appropriate for completion and collection, based on the risk posed by the software?
- Will unscripted testing (ad-hoc, error guessing, exploratory) or scripted testing (robust or limited) be performed, or both?

4. Establish an appropriate record

Does the record of CSA activity include the following?

- The intended use of the software feature, function, or operation
- The determination of risk of the software feature, function, or operation
- Documentation of the assurance activities conducted, including:
  - » Description of the testing conducted based on the assurance activity
  - » Issues found (e.g., deviations, failures) and the disposition

- Conclusion statement declaring acceptability of the results
- Date of testing/assessment and the name of the person who conducted it
- Established review and approval when appropriate

The draft is full of example guidance for evidence capture and testing activity, and, assuming no dramatic changes in its final form, should set the tone for how regulated businesses adopt a sensible, efficient and risk-based approach to their computerized system assurance.

Read the draft guidance ›

Quality, not compliance

The shift to computerized system assurance is part of a broader trend being driven by industry bodies such as the FDA and ISPE.

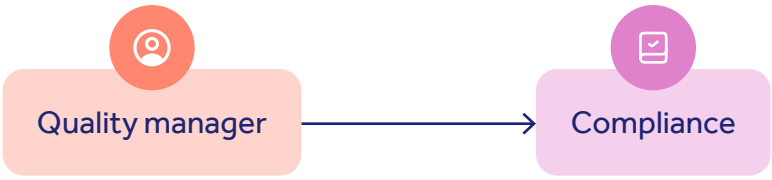
It's aimed at replacing a stressful, self-inflicted straitjacket of *compliance*-based CSV activity with measured, sensible, *quality*-based CSA actions.

As the Enabling Innovation Good Practice Guide puts it on page 9:

> ***As part of the Case for Quality Program, the US FDA CDRH (Center for Devices & Radiological Health) has identified that an excessive focus on compliance rather than quality may divert resources and management attention toward meeting regulatory compliance requirements rather than adopting best quality practices.***

The intended shift can be summarized as follows:

Current journey



01. Regulated business comes into existence and wants to bring a life science product to market

02. The company knows it must pass regulatory hurdles and inspections to do so

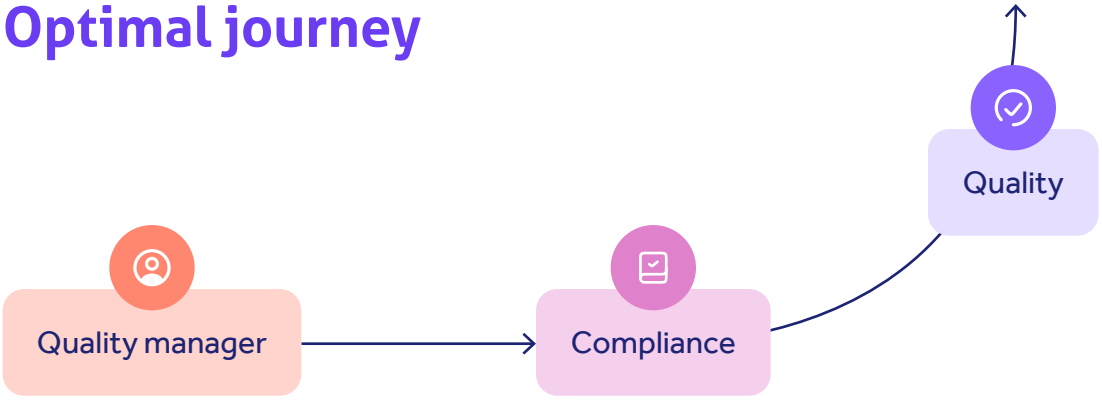
03. The company fixates on regulatory requirements and compliance needs, constructs its quality management system around these needs, and treats inspections as a stressful exam to be passed

04. Effort is spent on getting to the end goal of compliance and rigid clause-by-clause adherence. Fear of adopting computerized systems because of the extra burden of validation means the company either sticks with paper OR generates mountains of documentation in tandem with its computer system vendor to show to inspectors, such as installation, operational and performance qualification reports (IQs, OQs & PQs) and complex risk assessments

05. The auditor arrives and finds vast effort has been spent building validation packages for low-risk non-product computerized systems, such as an eQMS. Since there's no direct risk to patient safety from these systems, they don't want to waste time reviewing it. Meanwhile, high levels of paper and manual processes make it difficult to get the information they require to be confident the company is operating responsibly

06. In worse-case scenarios, the unnecessary one-size-fits-all attention given to low-risk systems has detracted from value-add activity and management of high-risk systems and processes. The auditor has plenty to note on his report!

Optimal journey



01. Regulated business comes into existence and wants to bring a life science product to market

02. The company knows it must pass regulatory hurdles and inspections to do so

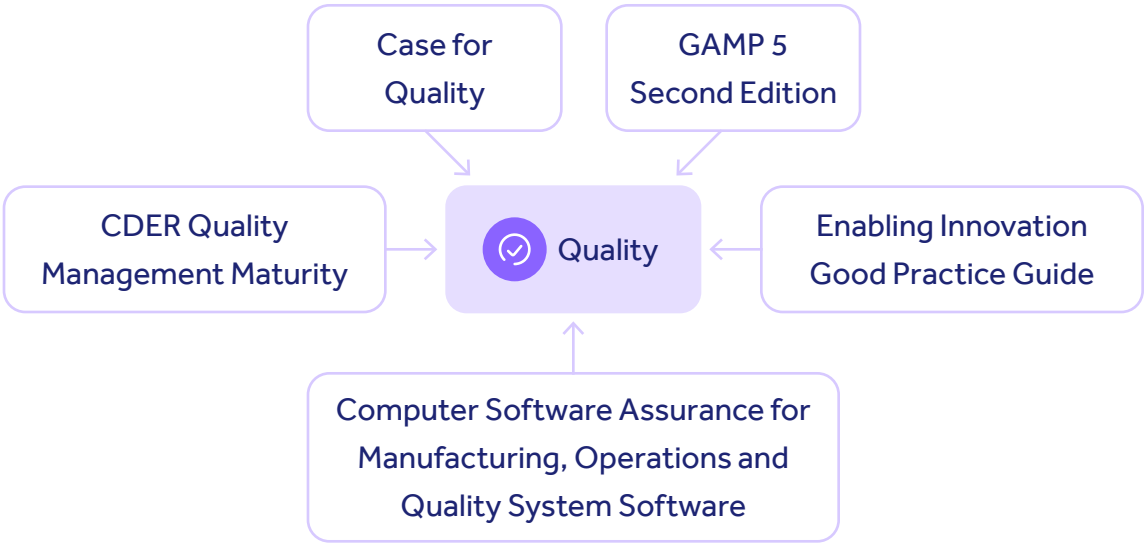
03. The company focuses on optimizing quality, managing risks, and adopting tools that will strengthen the operation and unlock these objectives. Its quality management system is built around continuously improving the safety of the patient and the end product, and treats inspections as an incidental learning opportunity on the path to market

04. Effort is spent on getting to the constant stretch goal of optimal quality, integrity and patient safety, using regulatory requirements as a stepping stone. Sensible risk-based assessment of eQMS platforms from established industry vendors means computerized system assurance can be performed quickly with minimal burden. Rather than generating an unnecessary protective layer of compliance documentation themselves, they can lean on the vendor's own testing activity and perform some additional testing if they feel it's necessary

05. The auditor arrives and finds appropriate effort has been dedicated to assurance of computerized systems dependent on their risk profile. The company has applied critical thinking, common sense and a risk-based approach to prove quality and compliance across the business. Because they've ditched paper, the auditor can access the data they need at the touch of a button. The quality manager has a stress-free audit experience, perhaps with a few learning opportunities

06. Eliminating fear-based compliance work means the auditor can detect clear value-add quality activity and strong management of high-risk systems and processes. The auditor is confident in the safety and integrity of the product going to the end patient, and might even be able to finish the inspection earlier than planned!

> ***Dr Janet Woodcock, former acting commissioner at the FDA, has been saying the same thing for decades: Don't primarily think compliance, think quality. Don't think, 'what would the FDA like?' Think, 'what would safeguard the patient and the efficient delivery of drugs?' If you do that, you'll keep them happy – rather than thinking the FDA wants you to produce all these documents so they'll give you an easy ride on inspections.***
>
> **— Sion Wyn**



A new approach to eQMS adoption

The evolution to computerized system assurance impacts how regulated businesses work with eQMS market vendors.

FDA and GAMP leadership want regulated businesses to strengthen their quality approach by replacing manual paper-based systems with electronic systems.

The new landscape of CSA therefore aims to make eQMS adoption as quick and painless as possible, without businesses subjecting themselves to an unnecessary and time-consuming validation headache.

Good, appropriate CSA work with a reputable eQMS vendor should therefore include these things:

1. IQs, OQs and PQs? RIP!

Installation, operational and performance qualification activity was 'borrowed' into CSV from older process validation frameworks in the 1990s, as the industry scratched around for a suitable CSV approach.

They remain appropriate for simple computerized tools, where a linear process of installing, checking operation and checking performance can be performed.

But the linear nature of IQ, OQ and PQ processes no longer matches modern, non-linear software development lifecycles – and tends to produce the kind of unnecessary paper documentation that regulators don't wish to see.

Their use in modern eQMS validation activity adds no value, and is symptomatic of the fear of regulatory punishment that the new world of CSA wants to stamp out.

> ***IQs, OQs and PQs are very ineffective in a typical large-scale modern software development or configuration environment… where those kinds of deliverables are just not a natural or useful part of the lifecycle. But we still have these really strange situations where acceptance testing is performed, then an OQ is added as a kind of 'layer', or user acceptance testing is performed and there's a document with ten signatures on to say that it happened. There's no reason you should have an IQ, OQ or PQ.***
>
> **— Sion Wyn**

The FDA's *General Principles* recognized that IQs, OQs and PQs are largely meaningless for software developers back in 1997, and didn't mandate them.

That remains the case in the 21st-century world of burndown charts, backlogs, regression testing, and other modern software testing activities. Automated testing tools like CircleCI and GitHub simply don't produce IQs, OQs or PQs.

Remember —
Any eQMS vendor you work with doesn't need to provide IQ, OQ or PQ documents to help you validate their system. Your FDA inspector won't ask to see them. And using them means you aren't adopting the agile critical thinking of modern CSA.

Watch video — Why you don't need an IQ, OQ or PQ for your validated system audit ›

2. Smarter testing

Regulated businesses adopting an out-of-the-box eQMS in the traditional 'compliance fear mode' can fall into the trap of performing unnecessary system testing to try and protect themselves from a future auditor.

Work with a vendor that doesn't encourage these activities and helps you get your system set up with minimal fuss and effort.

Typical mistakes include:

- Repeating testing activities already performed by the vendor
- Conducting tests on your own 'instance' of multi-tenancy software, where the results will be identical
- Testing by default whenever new software updates are rolled out
- (As we've seen) demanding IQs, OQs and PQs from your vendor

A reputable eQMS vendor will constantly test their software themselves, and assume the burden of the majority of assurance activity to prove their system meets your needs and intended use.

Perform your own testing only when your critical thinking approach suggests that a feature or new feature might reasonably impact product and patient safety.

Remember —
A good eQMS vendor will help you drive a sensible quality and regulatory approach. Encouraging you to perform non-value-add validation activity means they aren't prioritizing your real operational needs – and they probably haven't done their homework!

3. Sensible documentation

It's okay to lean on your supplier's provided documentation, especially if you aren't configuring your eQMS and are using it out of the box.

Focus any of your own additional testing and documentation according to:

- The risk level of operating your eQMS in your particular environment
- Functional requirements, not what you think your auditor will expect to see

The FDA doesn't prescribe the quantity or format of documented assurance evidence, precisely because it should be appropriate, risk-based and tailored to your specific use case.

The vast majority of the software development and testing is done as part of the eQMS vendor's *own* quality management system. That's why, according to Sandy Hedberg of USDM Life Sciences, a robust supplier qualification is all that's really needed for out-of-the-box systems, with extra *ad hoc* testing by you for any customized features.

The need for configuration specifications, traceability matrices and test plans will depend on your level of GxP risk and your level of configuration or customization, while effective evaluation of the methodology and tools of your eQMS vendor is key.

Only create assurance documents that are of real value to *you*. Key questions to answer if you perform your own testing are:

- What was the risk assessment?
- What did you test, and how?
- Who performed the testing, and when?
- What were the results?
- Were there any defects or deviations, and how did you deal with them?

A sensible, concise, preferably digital summary of this activity with a clear conclusion and treatment of risk will make your auditor happy – and critical thinking is the golden thread holding all this decision-making and documenting activity together.

Remember —
A reputable eQMS vendor performs and documents their system's assurance activity themselves, and should provide it to you as you go live. Use it as the core (and probably the majority) of your assurance records!

> *If an eQMS supplier is relying on a lot of paper and is up to here with IQs, OQs and PQs, then my critical thinking tells me that's not an up-to-date supplier!*
>
> **— Sion Wyn**

Breaking down the Enabling Innovation Good Practice Guide

GAMP's Enabling Innovation GPG was published in September 2021 to sit alongside the main GAMP 5 guidance. It covers 3 key topics:

1. Agile software

Underlines the modern agile nature of software development and how GxP-regulated businesses can adopt and implement modern digital tools to strengthen themselves.

2. IT service provider management

Service providers like cloud eQMS vendors are assuming more and more responsibility for the testing and assurance of computerized tools. As we've seen, this shifts the emphasis onto regulated businesses from *directly* performing validation tasks themselves to evaluating and assuring how IT vendors *indirectly* perform them on their behalf. The GPG breaks down how regulated businesses can evaluate vendor activity, find reputable providers, and use agreements and contracts to ensure the heavy lifting is done properly by the vendor.

3. Adoption of critical thinking to support the objectives of CSA and the Case for Quality

The Guide emphasizes the importance of ditching unthinking tickbox exercises and replacing them with full subject matter expert-led understanding of your processes, data flows and risks – and how your software's lifecycle and usage aligns.

> *It's a backwards world, entrenched in paper and with resistance to adopting new tools. SaaS can help you in your journey. You'll have a better result.*
>
> *The medical device industry feels like banking 20 years ago, when everyone was allergic to cloud SaaS products because of fear and bureaucracy. But now there are neobanks, and everything's changed.*
>
> *Embrace those companies leading the charge and who can provide you services you haven't had before. It's a good change.*
>
> — **Daniel Aragao**
> Chief Technology Officer, InVivo Bionics
> Qualio customer

The Second Edition of GAMP 5: what's changed?

The Second Edition of the ISPE's GAMP 5 computerized system guidance was released in July 2022, replacing the First Edition unveiled in 2008.

In keeping with the broad emphasis shift to agile, risk-based adoption of modern digital tools for GxP-regulated businesses, the Second Edition brought these key changes:

- Recognition throughout the text of the non-linear, agile nature of software development; iterative, incremental and exploratory nature of modern software emphasized over linear models like the waterfall
- Shift in emphasis from traditional documents like IQs, OQs and PQs to risk-based records of information held in appropriate systems
- Crystallization of the document around the concept of critical thinking, including guidance of key areas of computerized system adoption where critical thinking should be applied
- Update of development appendices focusing on URS and functional/ design specifications to reflect modern, agile software
- Appendix on electronic production of records updated to reflect the rise of cloud-based technology and blockchain, as well as to clarify new expectations around electronic records, signatures and audit trails
- Multiple appendices updated to reflect modern ITIL approach to software development, and to clarify links between key areas like change and incident management

- New appendix about blockchain and distributed ledger technology
- New appendix about AI and machine learning
- New appendix about use of agile within a GxP environment
- New appendix about modern infrastructure and infrastructure management, particularly the replacement of paper with automation and AI
- New appendix about critical thinking

Conclusion: 10 takeaways

01. Make quality your operational goal for computerized system adoption, not compliance

02. Don't waste time on unnecessary documentation like IQs, OQs and PQs

03. Your IT vendor assumes the bulk of the responsibility for assuring the quality and integrity of their systems – it's your job to assess and qualify *them*

04. Use critical thinking and risk awareness as the golden thread to inform you if you need to perform extra assurance activity, in *which* areas, and to *what* extent

05. Don't work with a vendor stuck in outdated validation activities

06. Don't be afraid of your auditor or inspector

07. Ensure you have in-house understanding of modern computerized system adoption to help you assess and work with suppliers

08. Proving you've thought about the relationship of your computerized system to the safety of your product and patient is your primary objective – indirect systems like an eQMS do not require the same level of assurance vigor as an adverse event MDR reporting system

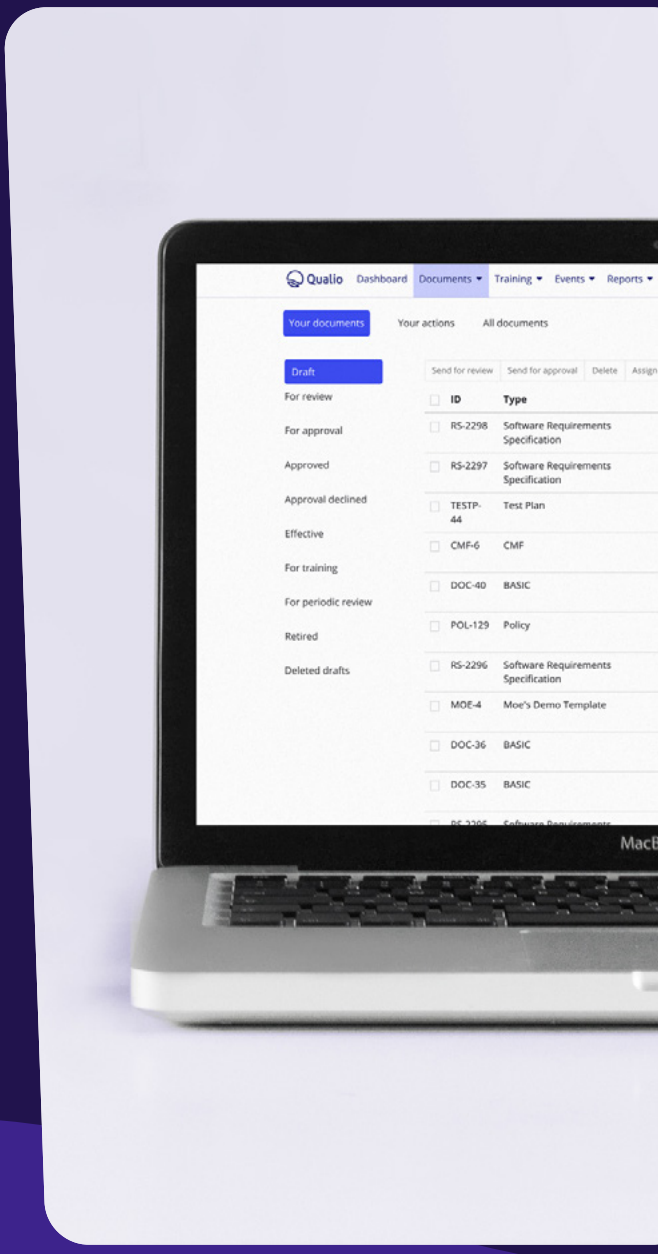
09. The FDA wants you to move from paper to computerized systems: it'll only make you stronger

10. Industry guidance, from the Case for Quality to GAMP 5's Second Edition, is remarkably consistent. Do your own reading and make yourself an expert!

Qualio

Ask us about our software assurance approach

Schedule a demo with us



Call us today
1.855.203.2010 • +353 1 697 1522