FINDING THE ASSURANCE in Computer Software Assurance

By Charlie Wakeham, Lorrie Vuolo-Schuessler, and Siôn Wyn

Computer software assurance (CSA) has been discussed widely in industry over the past five years. While the principles are well understood and welcomed, until now some of the practical detail on how exactly to implement CSA into an organization has been missing.

This article reaffirms CSA's background and alignment with published GAMP® guidance. It discusses the results of the workshop "Computer Software Assurance: Next Steps for Better Compliance" conducted at the 2022 ISPE Annual Meeting in Orlando, Florida. Finally, it delivers a practical analysis of the organizational changes and mindset needed to successfully implement CSA, critical thinking, and improved risk management.

CSA WORKSHOPS

In a GAMP® South Asia webinar in March 2024, only 14% of the 71 respondents claimed a strong understanding of CSA, with 31% having no prior knowledge (see Figure 1). The remaining 55% were unclear around the differences between CSA and computerized systems validation (CSV).

ISPE developed a two-part series on CSA in conjunction with the Society of Quality Assurance (SQA). The first workshop, in September 2022 and titled "SQA-CVIC and ISPE joint Workshop on CSA," was attended by 60 industry members. The second, in October 2022, took the output from the first workshop as the starting point for further investigation and brainstorming.

The second workshop was hosted by the following presenters (affiliations current at the time of the events):

- Charlie Wakeham, ISPE GAMP
- Lorrie Vuolo-Schuessler, ISPE GAMP and SQA
- Petch Ashida-Druar, ISPE GAMP and SQA
- Joseph Franchetti, SQA
- Ken Shitamoto, ISPE GAMP and FDA Industry CSA team
- Khaled Moussally, ISPE GAMP and FDA Industry CSA team
- Mike Rutherford, ISPE Chair and ISPE GAMP

Over 80 industry professionals invested their time and expertise in Orlando to explore overcoming the perceived barriers of CSA adoption. Those solutions are presented in this article, along with our grateful thanks to the attendees of both workshops for their participation.

BACKGROUND ON CSA

The US FDA Center for Devices and Radiological Health (CDRH) Case for Quality program [1] and the associated guidance document, "Computer Software Assurance for Production and Quality System Software, Draft Guidance for Industry and Food and Drug Administration Staff" [2], promote a risk-based, product quality–focused, and patient-centric approach to computerized systems. This approach encourages critical thinking based on product and process knowledge and quality risk management over prescriptive documentation-driven approaches.

The draft guidance has been prepared by the CDRH and the Center for Biologics Evaluation and Research (CBER) in consultation with the Center for Drug Evaluation and Research (CDER), Office of Combination Products, and Office of Regulatory Affairs. It states that when finalized, the guidance will supplement the FDA's "General Principles of Software Validation Guidance for Industry and FDA Staff" guidance document [3].

The FDA's 21 CFR Part 11 [4] document, which is applicable to all FDA program areas, describes the FDA approach to CSV. It specifically refers to the general principles of software validation guidance and to GAMP guidance. It is natural and logical for FDA

Figure 1: **Results from GAMP South Asia survey question "What knowledge do you have of CSA?"**

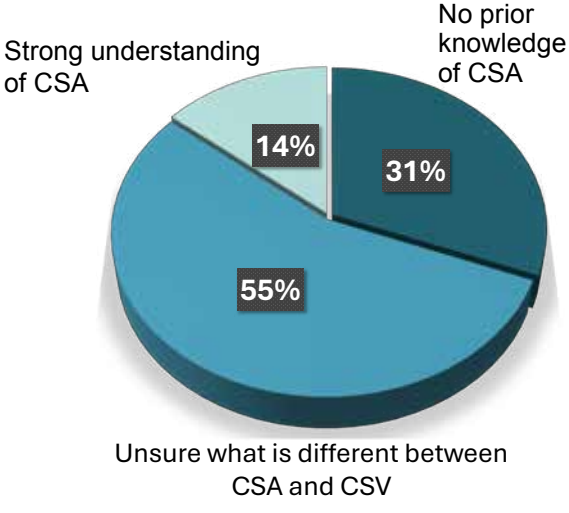
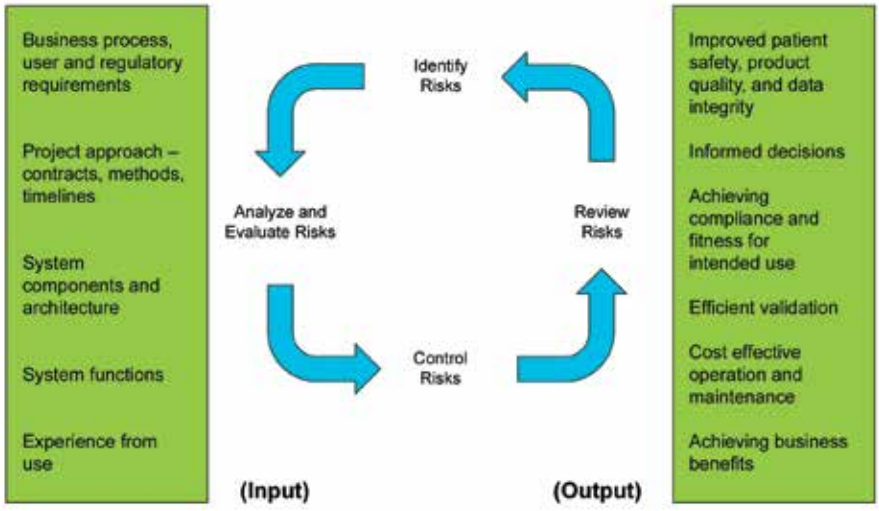


Figure 2: Overview and benefits of risk management [5].



centers to cross-refer to already existing guidance created by other centers rather than create their own. The guidance should not be seen as applicable only within CDRH or CBER program areas.

The ISPE GAMP Community of Practice and its global leadership strongly supports FDA's risk- and quality-based approach to the assurance of computerized systems, and believes that current ISPE GAMP guidance, and specifically *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition)* [5], is already fully aligned and consistent with such an approach.

We believe that the extremely valuable benefits and objectives of the CSA draft guidance can be fully achieved by applying *GAMP® 5 (Second Edition)*. This approach encourages critical thinking based on product and process knowledge, applies effective quality risk management over prescriptive documentation-driven approaches, and favors a focus on true quality over compliance. We judge that the draft guidance has already been very helpful in countering fears of perceived regulatory inflexibility that have traditionally contributed to outdated compliance practices.

We applaud the FDA's decision to apply modified terminology based on "assurance" to underline the fact that industry would greatly benefit from a change from old-fashioned, outmoded, paper-heavy compliance-focused approaches. A simple name change can be effective, as it draws attention to the fact that change is possible and desirable.

The use of the term "assurance" rather than "validation" is also logical as it is wider in scope and covers all the essential life cycle, operational, and governance activities involved. Current GAMP terminology is sufficiently flexible to support this thinking. The European Union, the FDA, and other regulations use the term "validation," but are not prescriptive on how this should be achieved. We believe that any detailed differences in approach or terminology are vastly outnumbered by the similarities in key concepts and shared objectives and benefits.

ALIGNMENT WITH GAMP

Here we highlight some key principles and objectives of the draft guidance and show how they are supported by and aligned with the GAMP approach.

The draft guidance reminds us that testing alone is not sufficient to establish confidence that the software is fit for its intended use. It recommends a "software quality assurance" focus on preventing the introduction of defects into the life cycle. It also encourages the application of risk-based approaches for establishing confidence that software is fit for its intended use. This is completely aligned with the *GAMP® 5 (Second Edition)* life cycle and verification approach.

The draft guidance supports flexibility and agility by encouraging regulated companies to select and apply the most effective testing approaches for various circumstances, together with continuous performance monitoring and data monitoring in operation, as well as leveraging various activities performed by other entities such as suppliers and service providers. This is fully aligned with the GAMP verification and testing approach and the *GAMP® 5 (Second Edition)* key concept of leveraging supplier involvement [5].

The draft guidance recommends focusing on features, functions, or operations that support areas of high-process risk, rather than those that do not pose a high-process risk. Failure to perform as intended not related to high-process risks would not result in a quality problem that foreseeably compromises safety, even though those other systems and functions are still regulated. This is supported by and consistent with *GAMP® 5 (Second Edition)*, Section 5.2 Science-Based Quality Risk Management, and reflected in Figure 2 [5].

The draft guidance reminds us that when deciding on the appropriate assurance activities, regulated companies should consider additional controls or mechanisms in place throughout the quality system that may decrease the impact of compromised

Figure 3: Session topics within the workshop.



safety and/or quality if failure of the software feature, function, or operation were to occur. Examples of controls and mechanisms include:

- Technical and procedural controls for the production process and the integrity of the data generated within that process
- Processes for assessing, selecting, managing, and monitoring suppliers and service providers, including assessment of software supplier quality and life cycle activities
- Data and information periodically or continuously collected for the purposes of monitoring or detecting defects, issues, and anomalies in systems after implementation
- Life cycle management tools (e.g., for defect logging and management, testing, performance monitoring, release, deployment, and maintenance)
- Testing performed in iterative cycles and continuously throughout the system life cycle

These are described and recommended in multiple GAMP guidance documents, including *ISPE GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition)* [5], *ISPE GAMP® Good Practice Guide: Enabling Innovation – Critical Thinking, Agile, IT Service Management* [6], *ISPE GAMP® RDI Good Practice Guide: Data Integrity by Design* [7], and *ISPE GAMP® Guide: Records and Data Integrity* [8].

The draft guidance recommends the maintenance of sufficient objective evidence to demonstrate fitness for intended use and outlines what is generally required. The expectations listed are easily achieved by following an appropriate *GAMP® 5 (Second Edition)* life cycle [5]. For example:

- The intended use of the software feature, function, or operation: Defined in Requirements and other Specifications
- The determination of risk of the software feature, function, or operation: Captured in a justified and documented risk assessment
- Records of the assurance activities conducted, including description of the testing conducted, issues found and disposition, and conclusions: Captured in test specifications, reports, and life cycle tools

Finally, the draft guidance pragmatically and helpfully reminds us that documentation of assurance activities need not include more evidence than necessary to show that the system performs as intended for the risk identified. It should also be sufficient to serve as a baseline for maintenance and improvements or as a reference point if issues occur.

WORKSHOP OUTPUT

The workshop at the ISPE Annual Meeting in October 2022 comprised four sessions. Each session contained three questions focused on related aspects of the session topics, which are shown in Figure 3. Multiple breakout teams addressed each question, and their responses are presented here with additional input from GAMP global leadership.

Session 1: Critical Thinking, Quality, and CSA

Question 1: How can critical thinking become fundamental and utilized routinely throughout an organization?

For an organization to understand the value that critical thinking can bring to their operations, it's key to first develop a quality culture in which quality, information technology (IT), validation leads, and the business process owner(s) fully understand and embrace their roles and responsibilities to collaborate effectively. The quality culture should enable management to lead by example and drive a culture that questions the standard approach, breaks down organizational silos, and allows flexibility in approaches. Critical thinking should be prioritized through training initiatives and recruitment.

To institutionalize the incorporation of CSA and critical thinking, the entire organization must be trained in the value and purpose

of including critical thinking and risk management principles in all activities. Critical thinking and risk-based approaches then become operationalized as integral parts of the company's culture.

System-level risk assessments and functional risk assessments should be included in each project and include quality, IT, validation leads, and the business process owner(s), along with appropriate subject matter experts (SMEs) as needed. The risk factors associated with the particular product and process may be specific to that combination. These should be reflected in the assessment when considering the impact to both the patient and the business if the risk occurs.

Incorporating critical thinking into a process is intended to strengthen the controls and robustness of the process, not to offer shortcuts. It should not be misused to that end.

Question 2: How do we get company leadership, and especially the quality function, onboard and supportive of CSA concepts?

GAMP® 5 (Second Edition) defines the CSA concepts in clear terms positioned within the life cycle and should be the roadmap for any organization wishing to adopt these practices [5].

The benefits of CSA may be best achieved with the use of software tools supporting the life cycle (e.g., requirements management and automated testing tools). It may be challenging for an organization to move away from paper and "paper-based thinking" and adopt electronic workflows. An understanding of the potential efficiency gains with software tools and leveraging artifacts in the place of traditional documents can support this move.

However, it is important that an organization understands that investing in tools does create an increased upfront cost. Though, once implemented and adopted, the CSA approach should deliver a highly defensible system with reduced long-term cost.

CSA is an evolution of software validation, and the role of quality must evolve accordingly to bring their knowledge and expertise into this more flexible and adaptable approach. The quality function will transform from the gatekeepers (i.e., as essential approvers on formal documents) into stewards of life cycle activities. These stewards ensure the life cycle activities are consistent with the validation strategy and provide strong assurance of fitness for intended use.

Increased patient focus and critical thinking can optimize the assessment of requirements and increase effectiveness and coordination internally and between regulated companies and vendors.

Question 3: How does a culture of quality vs. a culture of compliance support the organization?

A culture of quality is one in which the focus is on producing the right evidence for critical areas. This is done with the goal of producing a system that is fit for use in the business process that it supports, inherently delivering both quality and compliance. It is supported by collaboration, critical thinking, and a risk-based approach focusing on ensuring patient safety, product quality, and data integrity. Conversely, a compliance culture focuses on meeting perceived regulatory expectations based on completing a fixed set of universally applied predefined activities for each system, without any assurance of consistently achieving quality. A quality culture can only be established within an organization when driven by a committed management team. It is important in such an organization that everyone recognizes quality as part of their job, that there is tailored training of all personnel, and that management focuses on rewarding behaviors that support the set goals. The use of multidisciplinary teams and membership diversity in governance boards will facilitate and encourage collaborative working and clear accountability. This is essential to the quality culture.

Session 2: Vendor Management Practices and Audit Approaches for CSA

Question 4: After a vendor audit, how do you use the information gained and leverage that knowledge in planning your validation and ongoing control activities?

Many organizations are now partnering with vendors and wanting to leverage vendor documentation. So, vendor assessments, clear service level agreements (SLAs), and quality agreements are critical to the success of the engagement. Only with knowledge of the vendor's quality practices is it possible for the regulated company to leverage activities performed by the vendor, and thus avoid repeating activities.

The CSA approach focuses resources on performing risk-based activities to complement and/or supplement previous activities where needed. The type and frequency of vendor assessment activities, including what follow-up and ongoing surveillance are needed, should be based on the product/services' intended use and associated risk. The information gained during the vendor assessment allows the regulated company to decide what level of confidence they have in the vendor's quality management system, life cycle, and records.

After an audit or vendor qualification, the regulated company may decide that the vendor does not have a sufficient quality system or knowledge of the industry and that they will not use the vendor. Alternatively, the regulated company may decide to proceed with using that vendor but establishing additional mitigating controls based on a thorough understanding of the business process and a documented risk assessment. A follow-up assessment can be used to determine if the vendor actions post-audit have been sufficient to mitigate risks identified during the audit.

If the vendor has a well-established quality system, the regulated company can assess their controls and test rigor and coverage (e.g., via the traceability matrix) against the intended use of the system. This will help determine what activities are needed to supplement the vendor life cycle. It is important to identify, assess, and mitigate risks associated with differences between the tested vendor configuration and the intended use; the validation plan should be used to justify and describe the use of any vendor information or activities. An action plan is needed to mitigate any remaining risks.

A vendor audit should only be performed when the information gathered during the audit will result in changes to the activities performed by the regulated company.

Question 5: How do you audit vendor testing in the system planning stage when you haven't done the risk assessment yet and do not understand the system?

It is important that a risk-based vendor assessment is performed by SMEs from an appropriate team (e.g., quality, IT, validation leads, and the business process owner(s)) as needed. The team should be selected based on the types of risks associated with the system/process and should meet prior to the first audit session. During this meeting, they should agree on the key focus areas relating to the intended use of the products/services.

The audit objective should be to evaluate the quality and maturity of the vendor processes, including their testing processes, to identify how the regulated company's project activities will be impacted in response to the assessment findings. This should be done while recognizing that the detail of the vendor's testing may need to be revisited later in the project by the validation team.

Question 6: How can a vendor do things differently with CSA, and where can critical thinking and risk management take a vendor in terms of more efficient and effective testing?

It is important that a vendor focuses on software development life cycle elements and applies critical thinking from a product perspective. The vendor procedures should ensure that the rationale for decisions impacting their product life cycle (e.g., evolving requirements or revising test coverage) is captured and maintained ongoing and can be clearly understood by personnel from diverse backgrounds (e.g., IT, quality, or business).

Many vendors follow Agile methodologies, including the use of automated tools supporting the life cycle. Careful selection of the language used to connect the information and artifacts in the tools to GxP validation terminology can help avoid duplicating information into a document set.

Session 3: Leveraging Vendor Activities and CSA in the Operational Phase

Question 7: Having used critical thinking, risk management, and CSA approaches during the project stage, how does this impact the ongoing maintenance of the validated state through the operational phase?

The use of these approaches during the project stage will ensure a deep understanding of the system and its use in support of the business process when entering the operational phase. This understanding should make it easy to continue risk-based CSA throughout the life of the system.

Lessons learned during the project phase can be used to tailor the operational procedures and ongoing management of the system. The SLA and/or quality agreement with the support provider can be strengthened to specifically address any areas of concern and/or potential risks identified during the system implementation.

Consideration of changes in the operational phase should involve quality, IT, validation leads, and the business process owner(s), just as in the project stage. When it is a change to a software application, rather than a change to infrastructure or process, the vendor release notes should be scrutinized to understand the changes.

All changes should be evaluated based on the impact the change will have on the intended use of the system. The risk assessment needs to be revisited to identify those changes impacting functionalities determined to be associated with high-risk processes (including impacts to any other systems that integrate with this system). Critical thinking should be used to develop test plans accordingly, and ideally automated test tools should be in place to provide regression testing on high-risk processes after each upgrade or set of changes.

It is important to note that automated regression testing is a valuable and consistent tool for ensuring previously correct functionality has not been impacted by the change; however, it is also important to recognize that automated test cases by their nature are scripted. Therefore, they will only test the same paths on each execution.

Low-risk changes can be operationalized through procedural controls and implemented with minimal disruption to business.

Question 8: If a vendor uses a combination of scripted and unscripted testing as part of their life cycle, how much can you leverage this testing and in what situations, if any, would you need to repeat any of this testing?

All vendor testing is suitable for leveraging if the vendor has a robust quality management system that defines the risk-based approach to testing, including scripted and unscripted testing, and if the unscripted testing was applied appropriately. However, vendor testing using undocumented, unscripted testing or using only unscripted testing as a blanket replacement for scripted testing in the interests of speed and convenience would not be suitable for leveraging by the regulated company.

If the vendor quality management system is not robust, then it may be necessary to repeat certain testing to confirm functionality relating to high-risk processes. The regulated company should apply additional testing where the software is configured or customized and perform scenario-based testing using their internal processes and data to ensure the system operates as intended in their environment.

Question 9: With continuous integration/continuous deployment (CI/CD) approaches, especially for software-as-a-service (SaaS) offerings, frequent incremental changes to our infrastructure and applications are becoming the norm. How much can the change management and validation burden be lightened on the regulated user?

If the vendor is managing changes on behalf of the regulated company, a closer relationship and oversight are required. This is because the vendor is now able to impact the compliance of the system in use directly. More rigorous assessment and engagement

with the vendor's internal processes are needed. This is to ensure the validation and controls are adequately maintained and managed for both the application and infrastructure through any changes.

With appropriate SLAs or quality agreements in place with the right supplier, CI/CD can significantly reduce the regulated company's burden for change management and validation when combined with the right mindset, appropriate process, and automated tools. The operationalization of low-risk (standard/routine) changes discussed in question 7 becomes essential in this scenario. Vendors will work on different release cadences and notification periods, so the regulated company must understand and manage the risks and impact these have when working with multiple vendors and solutions.

Session 4: Measuring CSA Benefits and Moving Forward with CSA

Question 10: What metrics can quantify and optimize the benefits of CSA in achieving and maintaining computerized systems as fit for intended use?

First, baseline metrics on the current validation process are needed. This is to provide a benchmark against which any differences arising from CSA changes could be measured. These need to be captured based on projects completed prior to CSA changes.

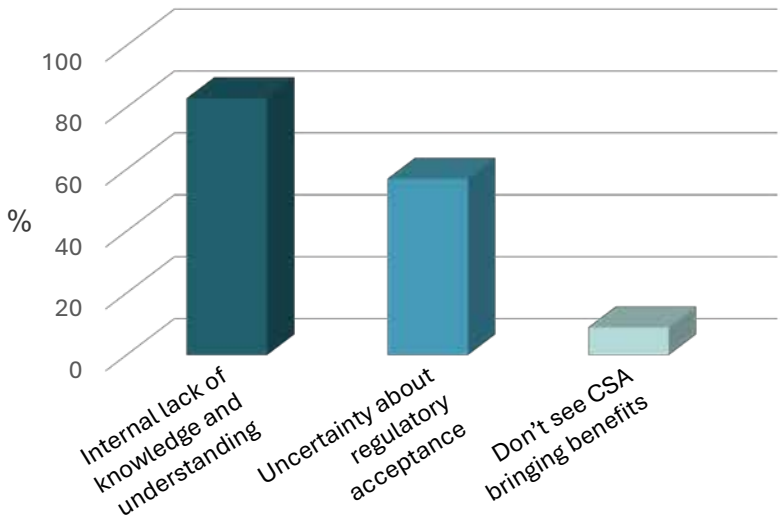
Second, both lagging and leading metrics should be used to capture process improvements and the effectiveness of a CSA approach. Examples of lagging metrics could include measuring the time to release a new system, level of validation resource used, duration of hypercare periods after a new implementation or major upgrade, number of deviations/incidents after go-live for functionalities associated to a high-risk process, and time to implement low-risk fixes/enhancements, with a reduction allowing an effective continual improvement program. These example metrics would all ideally decrease with an effective implementation of CSA approaches, risk management, and critical thinking.

Leading metrics could be based on items on a "punch list" of errors or issues to be added to the backlog and addressed in a future sprint. These could be predictive indicators of both the number of defects potentially within the software (high number of items on the punch list early in the testing suggests poor quality software) and of the amount of defect-resolution work still to be completed to close out the punch list items.

After a project, analyzing lessons learned and understanding the effectiveness as measured by the metrics could help optimize CSA approaches for future projects and releases. This is done by thinking critically about what updates need to occur to processes,



Figure 4: Results from GAMP South Asia survey "What barriers or challenges do you see to adopting CSA?"



systems, or records. Post optimization, the metrics should then show a corresponding further improvement.

Invest in software life cycle tools and training and use SMEs to ensure real understanding of risk management and critical thinking. This will help drive long-term success and efficiency gains. Companies need to understand the initial implementation cost of CSA (investment in software tools, upskilling, etc.) vs. the projected efficiency gains in the future.

Once the approach is fully implemented and matured, CSA benefits include process improvements that will reduce the incidence of issues in the operational phase. These will go hand-in-hand with improvements in the quality culture and the end product quality.

Question 11: What are the barriers to progressing with CSA and how can they be overcome?
Question 12: What can we do to confidently defend CSA approaches to other (non-FDA) regulators?

Note: Questions 11 and 12 are addressed together here, as the answers overlapped and complemented each other in a synergistic solution.

The concepts of the draft guidance are broadly applicable across all FDA-regulated areas, as discussed in the background earlier in this article. This applicability has led to the detailed inclusion of CSA approaches in ISPE's *GAMP® 5 (Second Edition)* [5], which applies to systems used in regulated activities under GMP, good laboratory practices, good clinical practices, good distribution practices, and good pharmacovigilance practices. *GAMP® 5 (Second Edition)* should also allay any fears that CSA is only acceptable to the US FDA and not to other regulators: GAMP guidance has provided a de facto standard for many years and has been accepted and referenced by regulatory agencies around the world.

CSA, as stated repeatedly by GAMP, is just a reinforcement of the risk-based approach. CSA builds on generally accepted principles of validation and fundamentally does not introduce a new way of working. This is because it aligns with the existing risk-based approach promoted since 2008 and recommended in the GxP regulations.

A more significant barrier to CSA adoption may come from the varied interpretation of CSA across industry (including regulated companies, vendors, and consultants) and regulators. In the April 2024 GAMP South Asia webinar, 83% of respondents cited the lack of knowledge and understanding of CSA within their own organizations as a barrier. This is compared to 57% being concerned about regulatory acceptance, as shown in Figure 4.

Again, GAMP guidance offers a common and pragmatic approach to implementing CSA and critical thinking; it can be used as the common interpretation. Investing in ISPE's training in GAMP methodologies and practices, as well as external training in critical thinking, will ensure a practical understanding of how to "do" critical thinking and how to capture and action the output of that critical thinking, i.e., the rationale for decisions and a risk-based approach. The increased understanding from such training will make explaining and justifying the validation approach during an inspection much easier to rationalize to regulators and other auditors.

There is unlikely to be a neat deadline by which all projects using the existing validation approach will be completed. Therefore, there will be ongoing projects using that approach running concurrently with newer projects using CSA approaches. Record the justification for the change in approach and demonstrate there is no decrease in control when transitioning from existing validation practices to new practices including, for example, the use of unscripted

Figure 5: Effective approaches for the implementation of CSA.



©2024 WakeUp to Quality Pty. Ltd. Used with permission.

testing. An inspection may include review of projects with existing practices or new practices. Both of these—when executed according to good practice and documented processes—should be acceptable to the auditor.

CONCLUSION

CSA is an evolution of software validation using a risk- and quality-based approach to assure that computerized systems and applications are fit for purpose. The outputs from the workshop series demonstrate that the tools and techniques are already available to support industry adoption, and this article provides practical advice on managed and effective approaches for the implementation of CSA at the leadership and operational levels, as shown in Figure 5.

As with earlier approaches, CSA should be applied to the full life cycle of a system. This life cycle includes development to implementation and operation and eventually system decommissioning and destruction. A computerized system life cycle is best holistically managed by a multidisciplinary team. This team includes SMEs from quality, IT, validation leads, and the business process owner(s).

CSA is neither an alternative for, nor a shortcut to, validation. It will require initial financial investment in life cycle tools and training, and early projects may consume more resources as personnel learn and adapt to the improved way of working. The long-term benefits of CSA done well—potentially shorter implementation times and less defects in the operational phase—will justify this initial investment. The focus of the CSA approach is on quality over compliance, giving an operational system that is fit for intended use within its business process instead of hiding behind excessive documentation.

Fundamental to an organization using CSA approaches is for them to create a quality culture and embrace critical thinking and risk management approaches in all their activities. Get critical thinking and risk management adopted and embedded into the organization, and CSA will naturally follow. An open mindset and willingness to embrace change, including implementing life cycle tools, are vital to success.

Some less mature organizations may experience resistance in implementing CSA due to the corresponding change in roles and responsibilities. The role of quality in the project will need to evolve from a gatekeeper mindset of reviewing and approving documents to a steward mindset, ensuring the activities proceed in accordance with the company's internal policies and provide guidance where needed in a flexible and versatile way to ensure regulatory requirements are satisfied.

CSA as a reinforcement of risk management complemented by a wider choice of test approaches and the use of life cycle tools can be implemented by, and bring benefits to, vendors, providers, and regulated companies. For a regulated company to be able to leverage vendor activities and build a long-term partnership, it is important they establish a robust risk-based vendor assessment process that drives and reinforces mitigation of any vendor risks identified during assessments.

Ultimately, the intention of CSA is neither resource saving nor efficiency gains but rather a substantial improvement in patient safety. Since *GAMP® 4* was published in 2001 [9], GAMP has promoted a risk-based approach to computerized systems quality. *GAMP® 5 (Second Edition)* provides updated, detailed, and pragmatic guidance on a computerized system life cycle approach using CSA and critical thinking as a reinforcement to the risk-based approach [5]. This article discussed, in detail, the challenges and practicalities around adopting the improved approach and how it can be achieved. Industry now has everything it needs to make the transition and find the assurance in CSA.

References

1. US Food and Drug Administration. "Case for Quality." Updated 29 July 2020. Accessed 22 May 2024. www.fda.gov/medical-devices/quality-and-compliance-medical-devices/case-quality
2. US Food and Drug Administration. "Computer Software Assurance for Production and Quality System Software. Draft Guidance for Industry and Food and Drug Administration Staff." September 2022. www.fda.gov/regulatory-information/search-fda-guidance-documents/computer-software-assurance-production-and-quality-system-software
3. US Food and Drug Administration. "General Principles of Software Validation. Guidance for Industry and FDA Staff." January 2002. www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles-software-validation
4. US Food and Drug Administration. "Guidance for Industry. Part 11, Electronic Records; Electronic Signatures—Scope and Application." August 2003. www.fda.gov/media/75414/download
5. International Society for Pharmaceutical Engineering. *ISPE GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems*. North Bethesda, MD: International Society for Pharmaceutical Engineering, 2008.
6. International Society of Pharmaceutical Engineering. *ISPE GAMP® Good Practice Guide: Enabling Innovation – Critical Thinking, Agile, IT Service Management*. North Bethesda, MD: International Society for Pharmaceutical Engineering, 2001.
7. International Society for Pharmaceutical Engineering. *ISPE GAMP® RDI Good Practice Guide: Data Integrity by Design.* North Bethesda, MD: International Society for Pharmaceutical Engineering, 2020.
8. International Society for Pharmaceutical Engineering. *ISPE GAMP® Guide: Records and Data Integrity*. North Bethesda, MD: International Society for Pharmaceutical Engineering, 2017.
9. International Society for Pharmaceutical Engineering. *ISPE GAMP® Good Automated Manufacturing Practice (GAMP) Guide for Validation of Automated Systems.* North Bethesda, MD: International Society for Pharmaceutical Engineering, 2001.

About the authors

Charlie Wakeham offers consultancy services and training in computerized systems quality and data integrity through her company WakeUp to Quality. She is the current Chair of the GAMP Global Steering Committee, leading the 5,000+ members of the GAMP Community of Practice as well as serving on numerous other GAMP and ISPE committees. Her career over 25 years has focused on GxP computerized systems and Quality. Charlie received the ISPE Max Seales Yonker Member of the Year Award in 2019 for her GAMP volunteer work and training of regulatory agencies. She joined ISPE in 1999.

Lorrie Vuolo-Schuessler received the ISPE Richard B. Purdy Distinguished Achievement Award in 2023 in recognition of her 20-plus years of contribution to ISPE and GAMP, including most recently serving as Chair of the GAMP Americas Steering Committee. She has co-authored multiple GAMP guides and articles and, despite having retired from her industry role as Senior Director Computer Systems Quality and Data Integrity at Syneos Health in 2022, Lorrie continues to actively contribute to GAMP through Special Interest Groups and Steering Committees and delivers GAMP training courses on behalf of ISPE. She joined ISPE in 2002.

Siôn Wyn is an international expert in computerized system validation and compliance and data integrity. He was a consultant to US FDA during the reexamination of 21 CFR Part 11, and a core member of the team that produced the FDA Guidance on 21 CFR Part 11 scope and application. He received the FDA Group Recognition Award for his work on Part 11. He also received the 2006 ISPE Professional Achievement Award, which honors an ISPE member who has made a significant contribution to the pharmaceutical industry. Siôn is a founding member of GAMP. He joined ISPE in 1995.

