REMOVING THE FRUSTRATION from Functional Risk Management

By Chris Reid, Sion Wyn, Charlie Wakeham, and Heather Watson

ISPE GAMP® 5: A Risk Based Approach to Compliant GxP Computerized Systems (Second Edition) [1], section 2.1.4 states "Quality Risk Management (QRM) is a systematic process for the identification, assessment, control, communication, mitigation, and review of risks."

ISPE GAMP® 5, Second Edition [1] states that, "Controls are developed to reduce risks to an acceptable level. Implemented controls are monitored during operation to ensure ongoing effectiveness."

Risks may be managed by elimination by design, reduction to an acceptable level, and verification to demonstrate that risks are managed to an acceptable level. Examples of risk control measures include designing failure detection mechanisms, implementing procedural monitoring, and testing to demonstrate that controls are fit for intended use.

The International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use (ICH) harmonized guideline "Quality Risk Management Q9 (R1) [2]" defines two primary principles of QRM:

- "The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the protection of the patient.
- The level of effort, formality, and documentation of the quality risk-management process should be commensurate with the level of risk."

We can derive from this that effective risk management is dependent on product and process understanding, critical thinking, and an understanding of how a computerized system supports the process.

PLANNING RISK ASSESSMENTS

QRM focuses effort where there is greatest risk to patient safety, product quality, and data integrity. However, experience shows that, too often, risk assessments are purely formal documentation exercises that have limited influence on the computerized system design or the implementation of controls to manage risk. There are a number of considerations when planning the risk assessment approach.

The value of risk assessment is limited by, for example:

- Failure to
  - include subject matter experts with product and process understanding who can clearly define the severity of a process or functional failure or who have the ability to detect a failure.
  - include subject matter experts with the appropriate system or technical understanding who can assess technical complexity and the probability of process or functional failure.
  - define appropriate mitigating actions to reduce risk.
- Risk assessments that are
  - conducted too early, so information is not mature enough to make valued judgement about risk.
  - conducted too late, so there is reluctance to modify design or conduct additional testing to reduce risk.
  - conducted against off-the-shelf functionality that implement industry best practice processes.
  - too granular (e.g., every single requirement is assessed rather than a feature area).

Scaling

High-level risk assessments conducted against processes or application modules can determine whether there is any patient safety, product quality, or data integrity risk. For example, this would include determining whether a finance module has any GxP risk. Processes and/or application modules that have no GxP impact are excluded from more granular functional risk assessments.

Lack of subject matter expertise

Even with the best-designed risk assessment process, a lack of subject matter expertise will lead to an erroneous outcome.

Process owners have process and product understanding and are best placed to determine the severity of risk scenarios. Functional experts have technical understanding of how the functionality is implemented and are therefore best placed to determine the probability of failure.

Generic risks

A number of risks can be anticipated in advance and managed as generic risks, particularly the failure modes. As such, it is not necessary to repeatedly evaluate generic risks. Table 1 provides some examples.

Granular or grouped requirements

Often, every single requirement is evaluated by the risk assessment. When requirements are written at a granular level, it is better to take a holistic approach and assess a related group of requirements, processes, or feature areas. In such cases, the primary risks requiring control can be identified rather than determining unnecessary controls for each specific requirement.

ISPE GAMP® Good Practice Guide: Enabling Innovation – Critical Thinking, Agile, IT Service Management [3] section 2.3.1 stresses the importance of logically grouping requirements in a structured manner. This approach significantly helps with the assessment of related requirements as a feature area or process area. (Note: it may be beneficial from a business perspective to conduct more granular risk assessments.)

Software/configuration error

Risk assessments often record "software/configuration error" as a risk scenario. This is the cause of the failure and is a superfluous and obvious statement. The failure scenario should clearly state how patient safety, product quality, or data integrity could be impacted.

Off-the-shelf solutions

Off-the-shelf solutions are designed by vendors to reflect industry best practice. Solution evaluation should confirm that this is the case. The likelihood of failure is low for mature off-the-shelf solutions. Therefore, for such solutions, the primary focus should be to determine functional severity to define the scope of validation effort. Assessment of probability of failure and detection mechanisms will be of limited value.

Novel solutions

Novel solutions are typically new or innovative solutions that may include limited process or functional understanding. It is essential that sufficient understanding is established before the risk assessment is started. As discussed previously, a risk assessment may evolve iteratively with the solution design. Process owners may require training to better understand the solution prior to commencing risk assessments.

INTEGRATING RISK ASSESSMENTS INTO THE DESIGN PHASE

Risks may be initially evaluated against business processes and/or requirements. However, for complex systems, risks should be further evaluated during the design and configuration phase. Additional information provided by design and configuration records is useful in confirming risk assessments or in revising to address additional information relating to detectability or the likelihood of failure.

Table 1: Examples of anticipated risks.

Feature	Generic Failure Scenarios
Data Interface	Data transfer does not trigger when required Data transfer does not recover following interface failure Data is incomplete Data is not loaded/mapped correctly
Reports	Report layout is incorrect Data is incomplete/incorrect Data resolution is incorrect/inaccurate Report is not generated when required Report is not saved Report is not approved
Data	Data entered by unauthorized person Data entered out of range Data not saved Data not stored accurately or in wrong data item Data approved by unauthorized person Data accessible by unauthorized person Data not protected against loss

Inform Design

Risk assessments are often conducted as a separate activity from process and functional design. As such, risk assessments are used to assess rather than to inform the design. Risk assessment should be an integral part of the design, where the risk assessment evolves with the design to establish a robust solution, rather than being handled by a separate team that conducts the risk assessment to challenge a completed design.

Agile frameworks cater to this very well when the risk assessment is an integral part of user story development, and when it is built into sprint planning, sprint review, and sprint retrospective—when the current risk conclusions and selected controls are developed and continuously monitored.

Evaluate Controls

Often the focus of risk assessment is to formulate test plans and test scenarios. The primary focus of risk assessment should be to ensure the designed controls are adequate. Testing is then used as one approach to verify that designed controls function correctly.

Consider Different Designs

For complex solutions, a different design or configuration may be used to deliver the same requirement. For example, this would

Table 2: Components of a risk assessment.

Risk Assessment Component	Description	Considerations	
Severity	The potential impact on patient safety, product quality, or data integrity. • Direct impact: High • Indirect impact: Medium • Negligible or no impact: Low	When to evaluate?	When the process and/or user requirements are defined and understood
		Who should evaluate?	Process owners
		What does it tell us?	The potential harm
		When is it relevant?	Always
		What do we do about it?	• Scale the validation effort; higher severity leads to greater validation effort • Identify and/or design controls specifically to control the harm and to minimize the impact on safety and/or quality to an acceptable level
Probability/Likelihood of Failure	Software is more likely to fail if it is a new code or complex configuration. Out-of-the-box software is well proven and less likely to fail. • Non-configured off-the-shelf software: Low • Configured software: Medium • Customized software: High Note: These are guidelines only. Complex configuration could increase the probability, and low-complex custom software could be medium. Probability should also consider human factors/error.	When to evaluate?	During design and configuration
		Who should evaluate?	Functional subject matter experts (SMEs)
		What does it tell us?	Likelihood that the function will fail
		When is it relevant?	For solutions that have complex design and configuration
		What do we do about it?	• Lower the probability by verifying that the function works • Avoid customized solutions when possible • Design should consider human factors/error and minimize the probability of such errors (e.g., with data entry verification)
Detectability	Should the system malfunction, will it be readily detected? • Automated or procedural detection that specifically looks for the failure: High • Thorough observation and/or focused data review, including consideration of audit trails: Medium • Unlikely: Low	When to evaluate?	When process design is complete
		Who should evaluate?	• Process owners who understand how failures could be detected • Functional SMEs who understand how the detection functionality works
		What does it tell us?	• Whether there is a failsafe mechanism to limit the risk of patient safety, product quality, or data integrity • The detection mechanism should be verified
		When is it relevant?	Most valuable for high-severity functionality
		What do we do about it?	• Consider alternative detection mechanisms if the risk is high • Verify that the detection mechanism is in place and working

occur when deploying multiple releases to different organizational units for a corporate solution (e.g., enterprise resource planning). In such cases, it is possible that the severity, probability of failure, and detectability could change.

For example, if the same requirement applies to similar processes but different products of differing risks, the severity of failure may differ. If the complexity of the design and configuration is different, the likelihood and detectability of failure may be different. As such, risks need to be reassessed considering different product severity, design, and configuration.

DETERMINING PROBABILITY OF FAILURE

GAMP Guidance

ISPE GAMP® 5 (Second Edition) [1] software categories provide high-level guidance on the probability of functional failure and should not be taken literally. Category 5, Customized Software, suggests a high probability of failure. However, if the code comprises only 20 lines, then the probability is likely to be less. Similarly, configuration, especially on large corporate applications such as enterprise resource planning systems, may be complex and need to be considered as a high risk of failure. Input from functional experts is essential when considering the likelihood of failure.

CONDUCTING RISK ASSESSMENTS

Timing

Risk assessments are often conducted too early or too late, or they take too long to complete due to protracted discussions. Conducting risk assessments early without sufficient process and/or product understanding can lead to insufficient information to make valued judgements about potential failure scenarios and severity of failures. Further, assessing the likelihood of failure before solution design and configuration phases may mean there is insufficient knowledge to correctly evaluate the likelihood of failure.

Completing risk assessments late limits the influence of the risk assessment outcome on the solution design and testing. Risk assessments completed after design approval are unlikely to lead to design changes to lower the risk and are too late to input to test planning.

Testing

Risk assessments use testing against designed controls as a means of reducing risk. Testing confirms that designed controls are fit for intended use and reduce the probability of functional failure. However, risk assessments often simply state "to be tested in functional and acceptance testing," rather than stating the specific test objectives arising from the risk scenario. As such, test teams must rethink the outcome of the risk assessment to determine what needs to be tested.

Planning Considerations

There is no doubt that risk assessment in the context of wider risk management is essential to ensuring computerized systems that are fit for intended use. However, mechanical application of risk assessments without critical thinking can lead to a poor outcome that has little influence on the design and validation of a solution. Table 2 explains the different components of a risk assessment and other considerations, such as when and by whom the evaluation will be done.

MANAGING RISK ASSESSMENTS

Risk assessment is only an element of the risk management process. Controls must be verified and risks must be monitored to ensure the risk treatment is effective. As such, the risk assessment must be managed in a way that can be readily maintained as experience during the project and operational phase is gained. Thus, risk assessments might be managed within a tool or as an integral part of the solution design.

CONCLUSION

Risk assessment is essential if risks are to be effectively managed during the project and/or operational phase. However, the output of the risk assessment is of limited value if it is not conducted by a team with the necessary process, product, and functional understanding. Conducting risk assessments prematurely may lead to invalid assessment of the overall risk. Conducting risk assessments too late will limit the opportunity to address design flaws and effectively test processes and functionality.

Mature out-of-the-box functionality is unlikely to present a significant risk, and therefore risk assessment should focus on identifying functionality that impacts patient safety, product quality, and data integrity to scope the validation effort. Complex systems that require significant design and/or configuration should be assessed for the likelihood of failure and the ability to detect failures that might arise from the incorrect design or configuration.

An efficient risk assessment process conducted at an appropriate level by the right SMEs will significantly increase the likelihood of delivering a solution that is fit for intended use. Risk assessment is a means of evaluating the effectiveness of designed controls and, where necessary, taking action to lower the risk through designing, testing, or proceduralizing activities to lower the risk. Risk management is primarily a process for identification and control of quality risks. As stated by the US FDA, "our primary focus …[is] to minimize the risks to the public health" [4].

References

1. International Society for Pharmaceutical Engineering. *ISPE GAMP® 5 Guide: A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition)*. North Bethesda, MD: International Society for Pharmaceutical Engineering, 2022.
2. International Council for Harmonization of Technical Requirements for Pharmaceuticals for Human Use (ICH). ICH Harmonized Guideline "Quality Risk Management Q9 (R1)." Adopted January 2023. https://database.ich.org/sites/default/files/ICH_Q9%28R1%29_Guideline_Step4_2022_1219.pdf
3. International Society for Pharmaceutical Engineering. *GAMP® Good Practice Guide: Enabling Innovation. Clinical Thinking, Agile, IT Service Management.* North Bethesda, MD: International Society for Pharmaceutical Engineering, 2021.
4. US Food and Drug Administration. *Pharmaceutical cGMPs for the 21st Century – A Risk Based Approach: Final Report*. September 2004. www.fda.gov/media/77391/download

About the authors

Chris Reid is CEO of Integrity Project Solutions Limited. Chris started his career as an automation engineer, providing software solutions to the chemical and pharmaceutical industry. For the past 35 years, Chris has provided IT program governance and IT quality solutions to global regulated companies. He is a former ISPE Board Member and the Past Chair of ISPE GAMP® Global CoP Steering Committee. Chris currently serves on the ISPE Foundation Board, he is Co-Chair of the ISPE IT Infrastructure GAMP® GPG3 Task Team, and is a member of the GAMP® Global CoP Steering Committee. He joined ISPE in 2000.

Sion Wyn, Director, Conformity Ltd., is an international expert in data integrity and computerized system validation and compliance. He served as a consultant to the US FDA during the reexamination of 21 CFR Part 11 and the guidance that followed. He received the FDA Group Recognition Award for his work on Part 11. Sion was Co-Lead of the *ISPE GAMP® 5 Guide: A Risk Based Approach to Compliant GxP Computerized Systems (Second Edition)* and the *ISPE GAMP® Guide: Records and Data Integrity*. He is a member of the ISPE GAMP Editorial Review Board and the ISPE GAMP Global CoP Steering Committee, among other committees. He received the 2006 ISPE Professional Achievement Award and the ISPE UK Fellow Award in 2016. He joined ISPE in 1995.

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 over 5,000 members of the GAMP® Community of Practice, and she serves on numerous other GAMP® and ISPE committees. Her career of 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.

Heather Watson is Director of TenTenTen Consulting Limited based in the United Kingdom, providing advice and consultation on computer system validation-related matters, including inspection readiness. Heather has 30 years of experience in the pharmaceutical industry. She has served in several global roles in various functions at GSK, with her most recent role being Director of Computer Systems Quality Assurance. She is the immediate Past Chair of the ISPE GAMP® Global Steering Committee, and is the Chair of the ISPE GAMP Editorial Review Board. Heather was Co-Lead of the *ISPE GAMP® 5 Guide: A Risk Based Approach to Compliant GxP Computerized Systems (Second Edition)*. She has presented at ISPE Annual Meetings and has been the Chair of IT-related tracks at ISPE Europe Annual Conferences. She has been the recipient of ISPE Committee of the Year Awards for the ISPE GAMP® Global Steering Committee in 2016 and 2022 and the ISPE Europe Annual Conference in 2019. She joined ISPE in 2001.