VALGENESIS®

WHITE PAPER

Adopting a Risk-Based Lifecycle Approach to GxP Computerized Systems through ValGenesis

VLMS – with GAMP 5 E2 and CSA Perspectives

TABLE OF CONTENTS

INTRODUCTION

The drive toward digitization requires best-in-class digital tools to manage the intricacies of the transformed business processes — and gain the full potential of that transformation.

Expeditious strides in genetic engineering have manifested a spate of cures for unmet medical needs. With the emergence and rapid mutations of novel viruses like COVID-19, manufacturers feel the pressure to bring drugs to market faster while ensuring that product quality, patient safety, and data integrity are not compromised.

Despite these new challenges, validation remains the holy grail of the life sciences business. Historically, it has had a bad reputation, with some calling it a "necessary evil." The concept has been associated with endless testing, copious documentation, and tedious processes. Fortunately, times have changed.
Vendors now offer robust, purpose-built technology, such as the ValGenesis validation lifecycle management system (VLMS), that revolutionizes validation's role from burden to competitive edge. The truly paperless solution affords users greater control in today's constantly evolving manufacturing environment, which requires short switchover times in multiproduct facilities. The ValGenesis VLMS is fully aligned with the latest industry guidance and best practices.

This paper will explain the critical thinking approach to computer software assurance (CSA) and the need for a robust risk management program to meet evolving requirements and standards such as ISPE GAMP 5 E2. It will also highlight the advancements in technologies and methodologies shaping the life sciences industry, setting the stage for adopting Industry 4.0, the fourth industrial revolution, and Pharma 4.0. Lastly, it will outline how the latest release of the ValGenesis VLMS, which includes a Design Manager module with functionality that targets true risk management features aligned with new guidance (CSA and GAMP 5 E2), will help regulated companies meet those requirements and standards out of the box.

KEY REGULATIONS AND GUIDELINES

Computer Software Assurance (CSA)

The United States Food and Drug Administration's Center for Devices and Radiological Health (CDRH) has been working on the Case for Quality (CfQ) initiative since 2011. This initiative includes the CSA methodology, which is designed to help life sciences manufacturers achieve computer system validation (CSV) more easily.

Traditional CSV focuses on producing accurate, approved documentation to present to auditors, then testing, assurance needs, and finally, critical thinking. CSA flips the paradigm emphasizing critical thinking, assurance needs, testing, and documentation, in that order. CSA reiterates the need to apply risk-based thinking and a least burdensome approach to software validation. The adoption of new technologies is also encouraged.

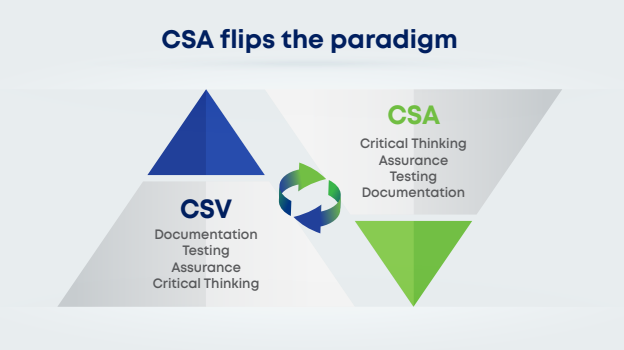

Figure 1. The Validation Paradigm Shift – from CSV to CSA

Similarities and Differences Between Testing Methods

Scripted Testing

Traditional validation requires scripted testing. A significant amount of time is needed to:

1. Develop the test script.
2. Perform dry runs to avoid deviations during actual validation.
3. Maintain the test scripts for any updates to requirements.

Qualified individuals, such as validation engineers, with education, experience, and training develop the test scripts. However, they may not be the end users. They are performing a quality control (QC) function, which is overseen by quality assurance (QA), on a system they may not understand, especially if the solution is new.

Therefore, developing the test scripts requires training on the system (or equipment, instrument, method, or process). The objective is to prove that the system consistently performs as intended and can identify invalid or altered records.

With scripted testing, the test script must be authored, optionally reviewed, and then approved (preapproval of a test protocol), likely with a QA signature, before executing the scripted test protocol. The protocol must be precisely followed. Any deviation must be recorded and processed according to the formal, effective procedure.

Ad Hoc Testing

The objective of ad hoc testing is to find errors and essentially break the system. Anyone can perform ad hoc testing; training is not a prerequisite. Preapproval of the protocol is not necessary. The challenge is to capture the objective evidence in case any challenges arise in the future during an audit or inspection.

Unscripted Testing

Unscripted testing is a type of software testing in which the tester is free to select any possible methodology to test the software. In unscripted testing, software developers rely on their learning, knowledge, skills, and abilities to test the software they developed.

> **Don't do things to pass a quality audit. Do quality things, and you'll pass an audit.**

Good Automated Manufacturing Practice (GAMP)

The International Society for Pharmaceutical Engineering (ISPE) released a new edition of the GAMP 5 guide in July 2022 (ISPE GAMP 5 E2). Like the FDA's CSA guidance, it reiterates the importance of applying a risk-based approach and critical thinking when defining how to address risk, such as what you must do if the risk is high versus medium or low. The latest GAMP guide and upcoming CSA guidance share many similarities. They state the same things in different ways.

The GAMP software categories, which are used to subdivide computerized systems according to complexity, have been useful to industry.

The categories have not changed since GAMP 5 E1:

- Category 1: Infrastructure
- Category 3: Non-configurable (i.e., COTS)
- Category 4: Configurable
- Category 5: Custom

NOTE: *There is no longer a GAMP Category 2: Firmware*

A Risk-Based Approach

A risk-based approach has always been preferred practice. It is included in both CSA and GAMP 5 E2 and is not necessarily new. In 2002, FDA released guidance advising regulated companies to take a least burdensome, risk-based approach to software validation. Unfortunately, the fear of negative regulatory findings caused organizations to adopt a risk-averse approach and consider (and validate) everything as high risk.

Over-validation unnecessarily taxed resources and cost the industry millions of dollars. Furthermore, risk management was incorrectly perceived as an early-stage task that only categorized items as high-, medium-, or low-risk. Once established and stamped, projects moved forward, and risk was forgotten. The assumption was that it had already been assessed.

Misconceptions about risk have persisted to this day. It is important for industry to understand that risk must be managed throughout the life of a system

MEETING CSA AND GAMP 5 2E REQUIREMENTS

A digital validation solution MUST support risk management as a lifecycle process to meet CSA and GAMP 5 E2 requirements.

Requirements Management

Requirements elicitation and development skills are often lacking. Good requirements are the essential building blocks of any system, whether it is a technology system, equipment, instruments, methods, or processes. Without good requirements, the system will not perform as intended. Thus, it cannot be validated and will not meet user needs. In other words, validation demonstrates that a system performs as intended. Intended performance is specified in requirements. Requirements originate with system users. Without knowledge of what users want or need, the system cannot be configured to meet those needs, making it impossible to demonstrate that the system performs as intended.

Risk management is a process, not a task. Identifying the risk category as high, medium, or low is just a start. Risk management must continue throughout a system's lifecycle.

GAMP 5 2E Requirements are Configurable Out-of-the-Box with the ValGenesis VLMS

Foundational system requirements needed to meet ISPE GAMP 5 E2 Standards:

1. *Assess the categories of software and hardware*
2. *System should support the lifecycle approach from design to risk-based validation*
3. *System development through Agile development approach, release management*
4. *Validation of high-risk requirements, change impact assessment, and retirement*
5. *Support the Agile approach*
6. *Computerized system validation framework – the system should support the system's validation along with the software*
7. *Support critical thinking for computerized systems*
8. *Quality risk management process for computerized systems*
9. *Managing changes efficiently with documented impact assessments*
10. *Validation of system development in an interactive (Agile) manner*
11. *System should support to validate high-risk requirements*
12. *Risk-based decision-making during test planning, operational, change control, and retirement*
13. *Determining risk-based system and functional assessment*
14. *Leveraging automated testing*
15. Periodic review

THE FOUR "C" OBJECTIVES

Several factors must be considered throughout the life of a system. Here are four:

- Compliant
- Consistent
- Complete
- Continuous

Compliant

The compliant objective signifies that the practice is compliant with the process, and the process complies with regulatory requirements, with the result always being quality output. ValGenesis technology helps users attain compliance through technical controls, programmatically and systematically, instead of relying upon humans to read and understand procedures. Relying on humans is risky because you cannot confirm that a procedure has been read and understood until the actual work has been performed. By then, it is too late.

With technical controls in a validated system, you can enforce processes and not have to wonder if someone really did read and understand a procedure.

Consistent

Processes and practices, as well as templates, controls, and procedures, must be consistent. Inconsistency results in unexpected outcomes; the inability to identify and correct problems, errors, and deviations; and compliance risks. All of which can jeopardize patient safety. A favorite technique among auditors and inspectors is visiting multiple locations and interviewing cross-departmental functions to identify inconsistencies. Problems are easily found nestled among these inconsistencies. With good technology, the only way to move forward is to follow a controlled process that includes quality checks and incorporates controlled templates and workflows approved by authorized users, including QA. ValGenesis delivers consistency through a host of leading-edge features, as this paper will demonstrate.

Complete

This objective is straightforward. If it is not complete, it is incomplete. The job is not finished. It is only complete if all areas are covered. If you are not looking at the entire picture, something will be missed, which can create a problem. Hard work will be lost. Therefore, the assessment must be complete. End-to-end and comprehensive are terms synonymous with complete.

Complete is the overall objective of risk management. To complete a risk management iteration, the risk must be eliminated. If it is impossible to eliminate the risk, it must be mitigated to an acceptable level. However, in some cases, there are no acceptable levels of mitigated risk, and risk must be eliminated. If it cannot be eliminated, it may be necessary to go back to the conceptualization and design phase or to consider removing the feature, function, or system altogether.

ValGenesis technology guides users through a complete process, allowing all factors to be addressed in real time. Templates developed by authorized users and approved by QA guarantee that standards are applied, and completeness is attained.

Continuous

This objective is where many companies fall short. Risk management or risk-based processes are often incorrectly seen as something to be performed at a project's beginning. This was mentioned above, but it's worth repeating. Risk management is a continuous process throughout the entire validation lifecycle, from the cradle to the grave – from inception to retirement. Systems develop, mature, break down, erode, improve, and degrade because everything is in a state of flux, including risk.

> **Throughout its lifecycle, the risk for a process, system, practice, or regulation will change, so risk must be assessed continuously.**

The VLMS with Design Manager innovation enables companies to manage risk by creating configurable risk matrices for severity and frequency. Users can tailor metadata related to each risk type and perform mitigation actions for each risk. The end of a flow cycle includes an action plan and risk control, that is, in effect, a feedback loop. This feedback loop is necessary to implement quality controls for the risk and constant monitoring, especially for high risk. This may, in fact, require another iteration of the lifecycle if controls are triggered.

Testing Methodologies

The ValGenesis solution supports any testing methodology. This is vital because a risk management process, through a risk assessment, must include an action to eliminate risk, or if elimination is not possible, mitigate it to an acceptable level. The system, feature, or function must be redesigned, or elements must be removed, if mitigation is impossible and risk is unacceptable.

> **Eliminate risk — that's the ultimate objective of risk management!**

Risk elimination and mitigation can be accomplished by implementing and testing risk controls. However, the Four Cs must be attained. The solution achieves this by leveraging templates, which are associated with content types. There is a direct correlation between content type and test methodology. For example, there can be an ad hoc, exploratory, or unscripted template. Similarly, there can be a content type for each of the additional test methodologies outlined below. Templates can also be developed for specific content types.

When performing a risk assessment, questions are raised, values are selected, and risk outcomes are determined. The system analyzes the risk outcome and applies business rules. A business rule can be used to assign content types.

After requirements are developed, testing is required. The system identifies the appropriate test methodology based on risk outcomes. This will be explained in more detail in subsequent sections.

Test Methodologies Commonly Used to Test Systems

The FDA identifies three new test methodologies in its CSA initiative:

1. Ad Hoc
2. Exploratory
3. Unscripted

Additional test methodologies include:

1. Positive
2. Negative
3. Performance
4. Security
5. Boundary
6. White box
7. Grey box
8. Black box

Performance testing tests the ability of the system to perform at acceptable levels. Security testing is conducted to ensure that the system is secure. Boundary testing confirms that boundaries, such as upper level of quantitation (ULQ) and lower level of quantitation (LLQ), as well as values near boundaries (including integers and decimal results) and values far beyond boundaries, are enforced.

THE VLMS DESIGN MANAGER INNOVATION

The solution follows a logical progression. Each stage will be described in detail, but first, it is important to understand the system prerequisites, configured as part of system implementation.

Prerequisites

Content Types

A content type is essentially a type of document. It could be a requirements document such as a user requirement specification (URS), functional requirement specification (FRS), or design specification (DS). It could be a qualification protocol such as an installation qualification (IQ), operational qualification (OQ), or performance qualification (PQ). The system also supports content types for validation plans (VP) and validation summary reports (VSR).
For each content type, there may be one or more templates. For example, a company can have several different types of IQ templates. There is a one-to-many relationship between content type and template.

Templates

It is common to find many different templates for a given content type. This is often required to address the specific needs of the testing, verification, qualification, or validation that is being performed. The system ensures consistency, so redundancy (duplicate templates for the same content type) is easy to avoid.

During configuration, content types are developed for the different testing methodologies:

- Scripted (traditional validation)
- Ad hoc, exploratory, unscripted (called out in new CSA methodology)
- Positive, negative, performance, security, boundary, white box, grey box, black box (commonly used)

Once the content types are established, templates can be developed for each type of content required, i.e., the different testing methodologies that will be leveraged based on the outcome of the risk assessment process.

Risk and Process Conditions

A risk process is configured in the solution to identify process conditions that will be applied. There is a direct correlation between process conditions and content type. There is also a direct correlation between content type and template. Ultimately, this means that a process condition may be associated with a type of content.
When there is an association (link) between process condition and content type, the content developed to test risk control, elimination, or mitigation is based on a compliant, standardized template.

A RISK PROCESS CAN HANDLE SEVERAL PROCESS CONDITIONS

Consider

- Negative
- Positive
- Performance
- Security
- Smoke

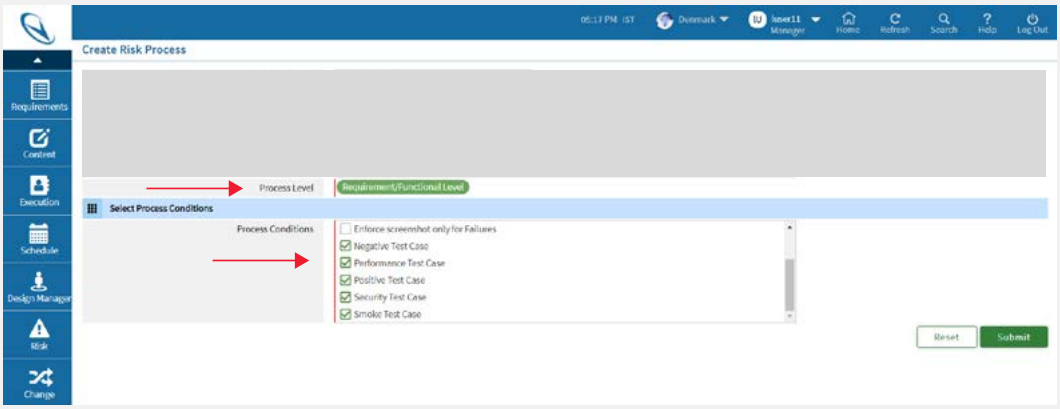

Figure 2. Risk Process and Process Conditions

Business Rules

Risk assessment results trigger business rules which are configured in the system. A business rule can have several outcomes (high, medium, low, critical, major, moderate, minor, or negligible) with different numerical results. When the risk assessment result falls within a given number range in a business rule, the process condition is triggered. The process condition enforces a content type which, in turn, dictates what template(s) is required for a test deliverable to verify the risk control and ensure it is eliminated or at least mitigated to an acceptable level.

Business rules assess risk score and invoke process conditions

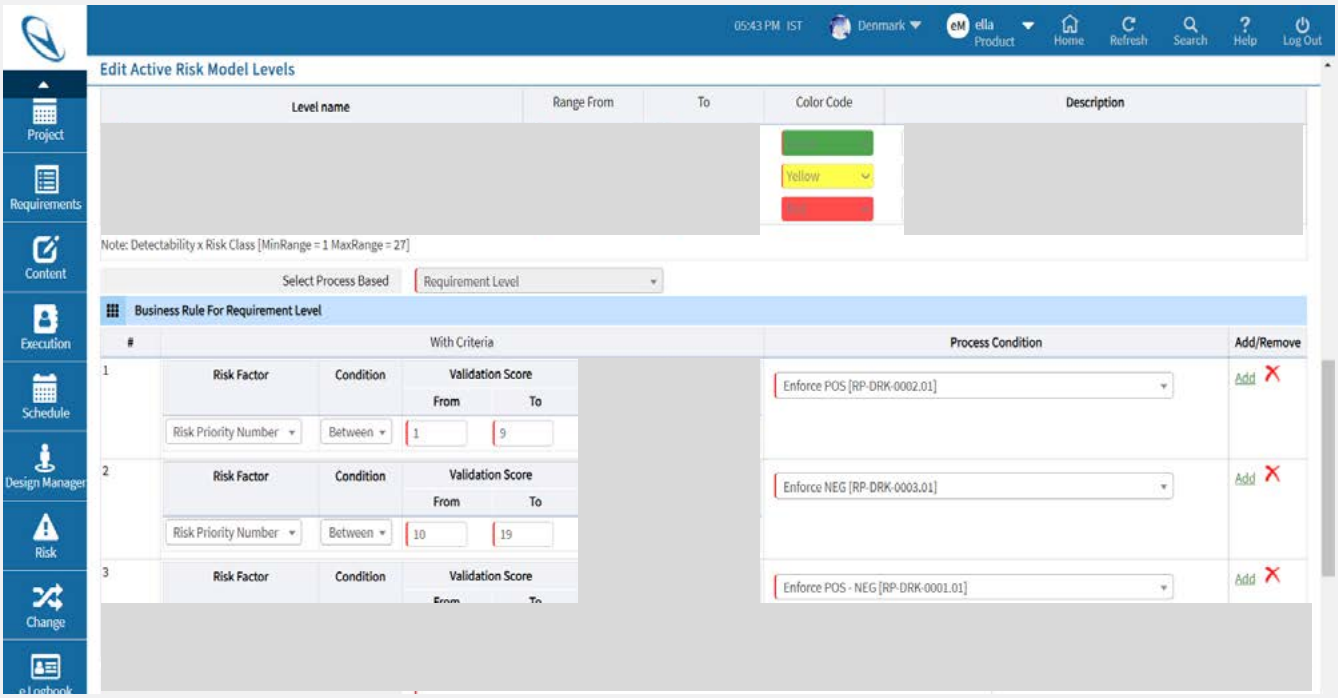

Figure 3. Business Rules and Process Conditions

Prerequisite Recap

Templates are used to perform a given type of test designed to verify that a risk is controlled, eliminated, or mitigated. These templates are associated with content types that define the different test methodologies or content deliverables. Business rules establish boundaries for different risk factor ranges. The process condition is enforced when a risk outcome falls within a risk factor range. Process conditions are associated with content types, and these are defined, as a prerequisite, as a risk process. Once the prerequisites are established during the initial configuration and implementation of the solution, the normal use of the system may commence. This is where the solution process flow kicks in.

Logical Progression of the Solution Process

Once the necessary prerequisites are in place, the solution guides users through six different stages, which are laid out in a logical progression.

Figure 4. Solution Logical Progression

Six Progressive Stages

Stage 1: Define

In the first stage, the risk framework, data to be captured, and processes to be performed are defined. The framework offers options in sequential order for the remaining stages:

- Criticality Assessment
- Failure Mode
- Risk Assessment
- Action Plan
- Risk Control

The risk framework identifies which of the above are to be included in the risk process. If one of the above items is included in the risk framework, it will be necessary to identify the data that must be captured at that stage. This is done by creating a template with form controls, such as a text box, text area, date/time picker, picklists, or radio buttons, to identify the data type and its corresponding label.

The requirement identification number and a requirement description are essential data elements. Everything else will be associated with this unique number and name.

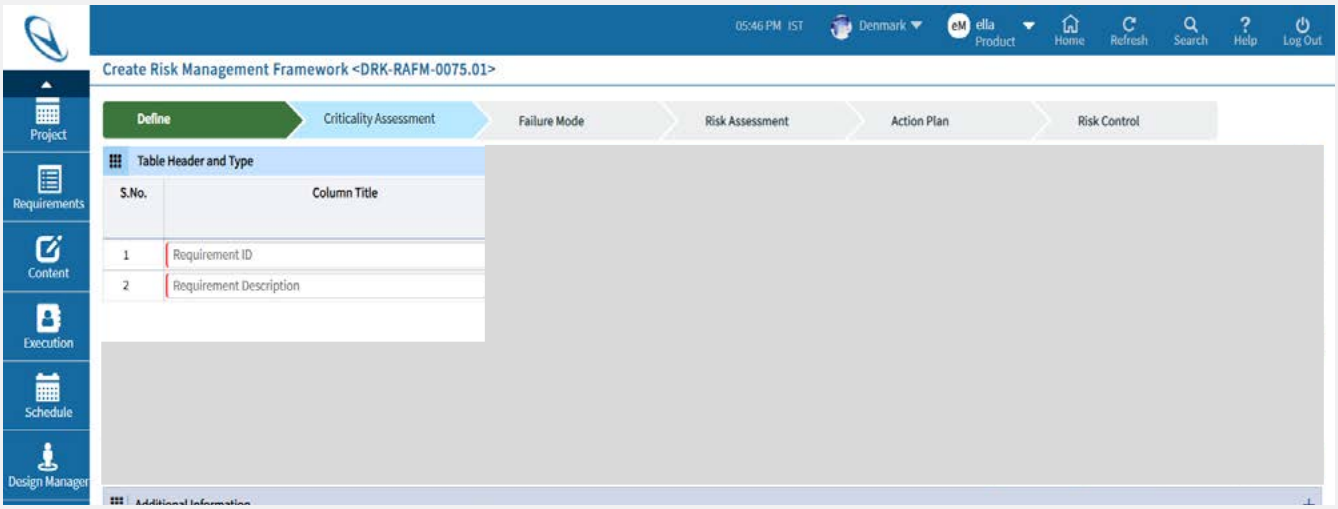

Figure 5. Essential Data Elements (Requirement ID and Requirement Description)

Stage 2: Criticality Assessment

The solution supports traditional risk models such as failure mode and effects analysis (FMEA), risk priority index (RPI), and risk priority number (RPN). It also allows users to create customized risk models with custom risk factors, calculations, derivative factors, and logic.

When performing a criticality assessment, a risk model is used with a business rule that determines what to do in response to a risk outcome. For example, suppose a criticality assessment determines that a system is critical. In that case, the system will instruct the user to perform a failure mode analysis followed by a risk assessment, create an action plan, and enforce risk control. In this stage of the logical progression, the risk model is identified along with the business rule.

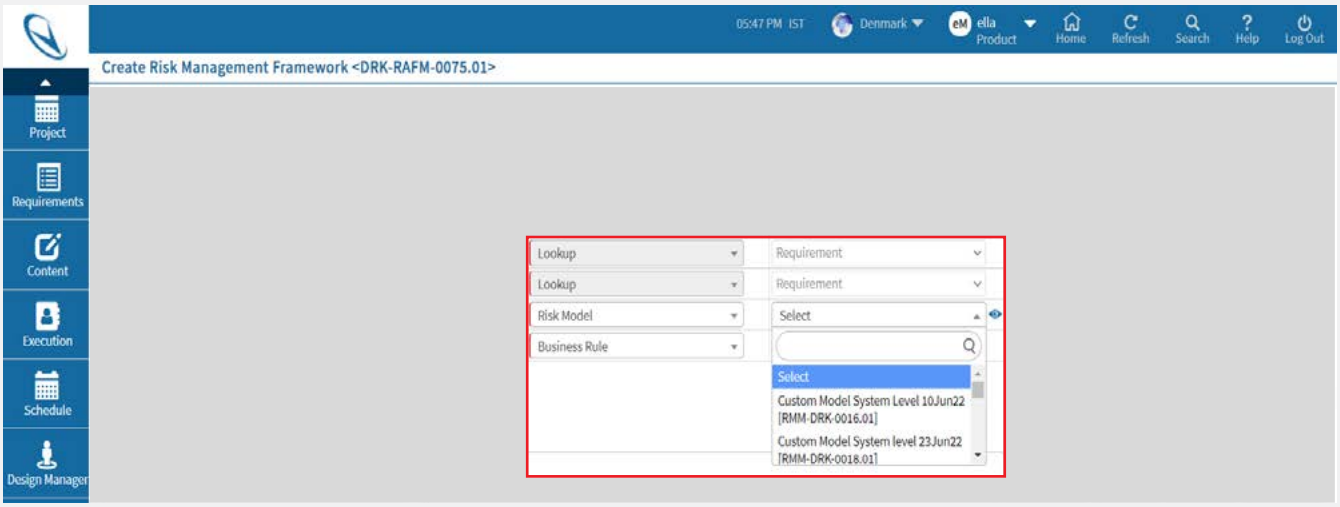

Figure 6. Risk Model and Business Rules in Criticality Assessment

With the details of the criticality assessment established, failure mode is the next stage, provided it is included in the risk framework.

Stage 3: Failure Mode

During this stage, every potential design failure is identified along with its cause and effect. If a system is considered critical, it is essential to look at all potential failures. Once all possible failure details have been identified, a risk assessment can be performed on each.

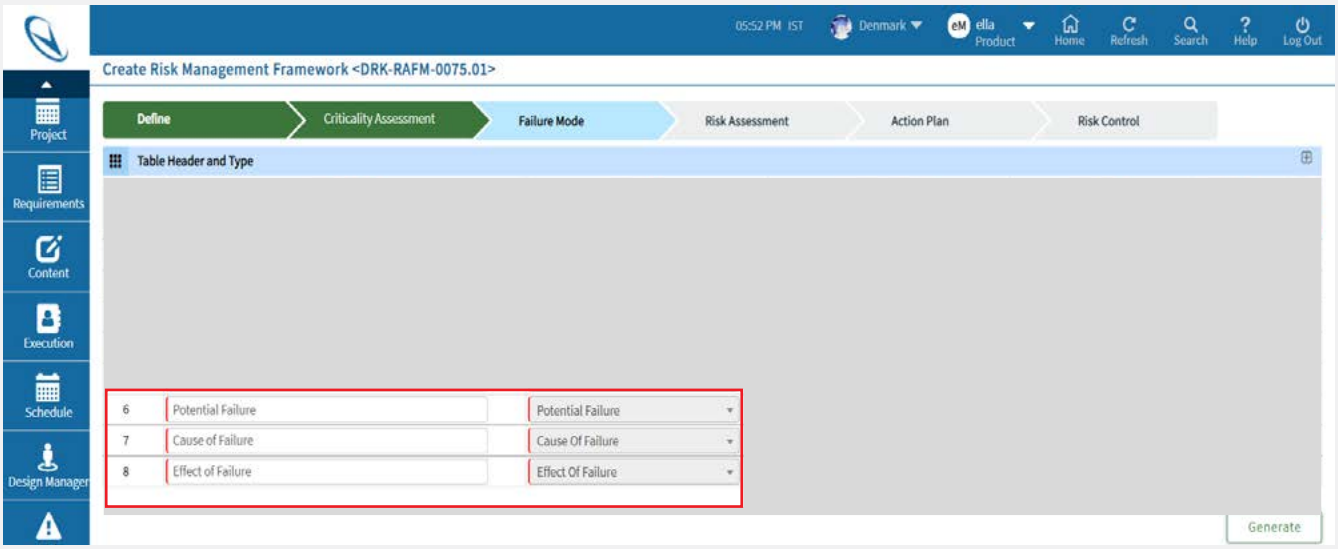

Figure 7. Failure Mode Stage

Stage 4: Risk Assessment

When performing a risk assessment, a risk model is used along with a business rule that determines what to do in response to a risk outcome. Multiple traditional risk models (FMEA, RPI, RPN) or custom models can be used. Depending upon upstream business rules, when a user reaches the risk assessment stage, one or more assessments may be needed for risk outcomes.

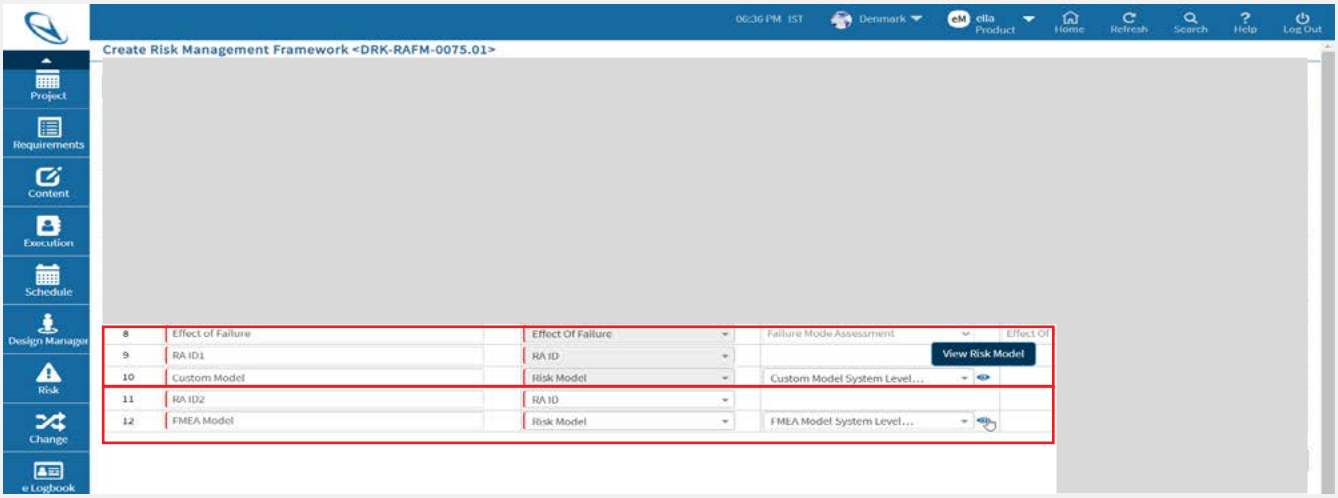

Figure 8. Risk Assessment Stage

With criticality assessed, failure modes identified, and risk assessments performed, the next logical step is to act.

Stage 5: Action Plan

This stage outlines what is required (planned) to control, eliminate and mitigate risks based upon the criticality of the system with all its potential failures. The action plan is where test methodologies (content types) are triggered based upon risks associated with individual requirements. For testing to commence, test protocols must be developed based upon standardized templates for a given content type. Positive, negative, performance or boundary testing may need to be performed. If the organization uses the CSA methodology, the risk level may allow for ad hoc, exploratory, or unscripted testing, especially if the risk is moderate or low. The same can be true for GAMP 5 E2 by following a risk-based approach. The point is that action must be taken.

Stage 6: Risk Control

The final stage is risk control. Risk management is a continuous process, and as such, it must be done at the beginning of a project and continuously throughout its lifetime. The ultimate purpose of identifying risk is to eliminate it. If a risk cannot be eliminated, the design of the feature, function, or system causing the risk must be reconsidered. In some instances, residual risk may be allowed if it is mitigated to acceptable levels. The purpose of this stage is to ensure risk is controlled throughout the life of the system. If it isn't, the loop starts again, beginning with stage one.

Relationships between Criticality, Failure Mode, and Risk Assessment

There is a logical relationship between criticality, failure modes, and risk assessments.
Figure 9 highlights this.

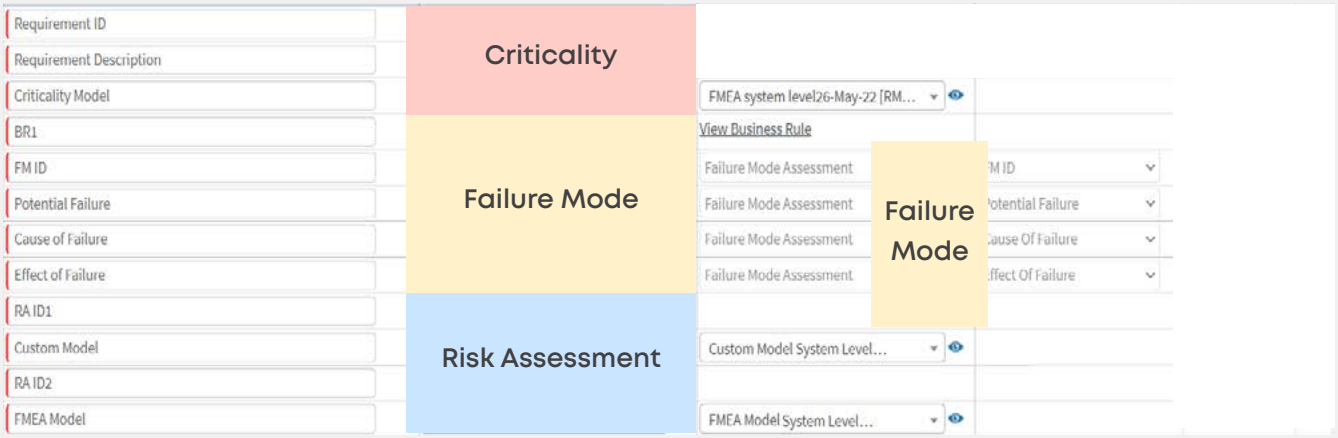

Figure 9. Criticality, Failure Mode, and Risk Relationships

VLMS technology maintains these relationships and enforces the logical flow of the progression. Companies can tailor the solution to meet their current and future needs with standard or custom risk models, templates, test methodologies and content types, business rules, and risk processes. Users can capture all information required for the different risk management processes applicable to their organization and its various systems. Comprehensive training and knowledge transfer during implementation give users the confidence to fully leverage the system's power and ensure a timely, successful implementation. The solution can be configured independently of ValGenesis. However, world-class professional services and technical support teams are always available to ensure that the system configuration meets the organization's core business requirements.

A Holistic View of Risk

ValGenesis' innovative VLMS Design Manager technology can perform requirement-level risk management, including criticality assessments and failure mode analysis, with corresponding business rule-driven risk assessments that support unlimited testing methodologies. It offers out-of-the-box support for CSA, GAMP 5 E2, and an efficient, least burdensome approach, fully leveraging the power of true risk management and an organization's unique requirements without needing any customization.

Figure 10 below illustrates how everything comes together in a comprehensive interface that provides a holistic view of a company's risk landscape across product lines and business processes.

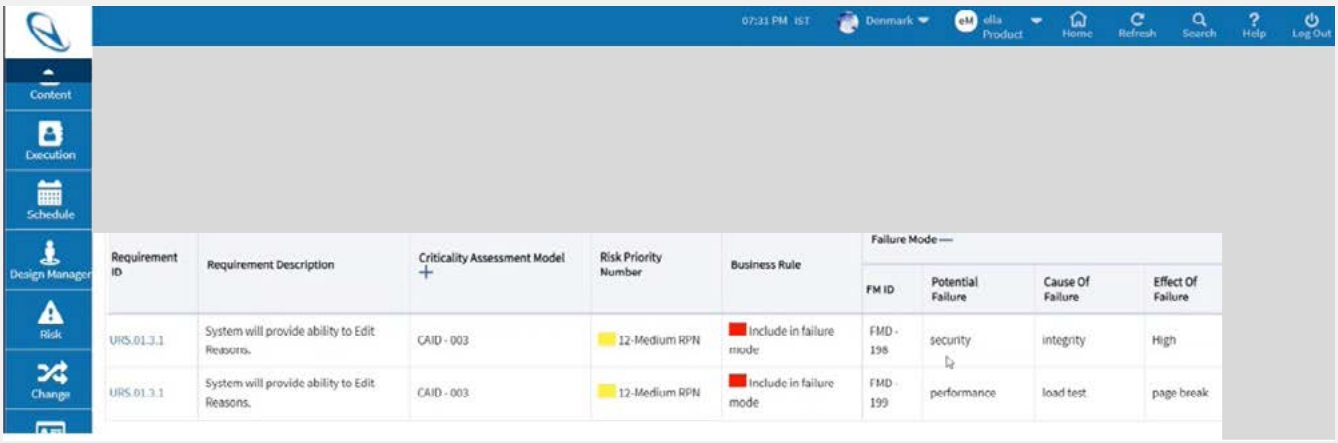

Figure 10. Automatic Criticality and Failure Mode Reporting

The solution will report risk outcomes with all relevant details in real time. The user determines what is relevant based on their needs, which are tailorable and configurable, and can implement controls with enforceable rules, logic, and standardized templates at a requirement level, including the ability to capture data elements they deem necessary.

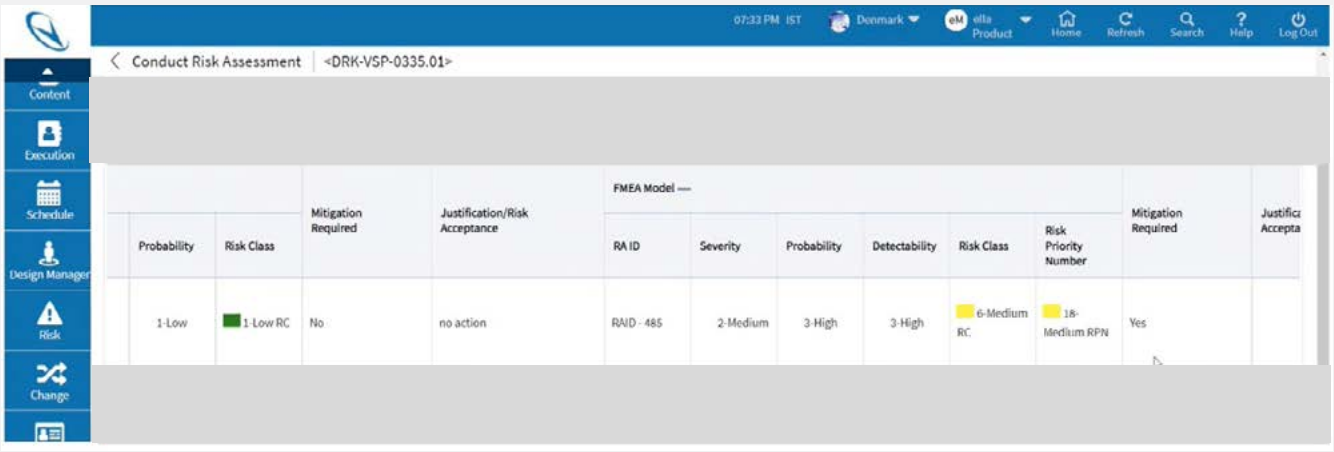

Figure 11. Holistic View of Real-Time Risk Outcomes

Automated Risk-based Trace Matrix Generation

ValGenesis is known for its ability to ease the frustration of paper-based requirements traceability matrix generation. Manually tracing these requirements on Microsoft Excel spreadsheets is highly error-prone and involves considerable time and effort. Design Manager can incorporate content types and corresponding test methodologies into the trace matrix. This allows users to strengthen their traditional validation efforts with enhanced testing methodologies following a risk-based approach that adheres to the Four Cs (compliant, consistent, complete, and continuous).

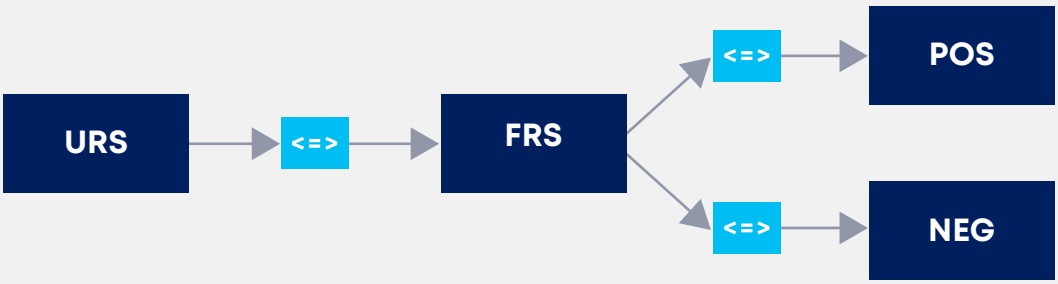

Figure 12. Trace Matrix including Multiple Testing Methodologies

With the advance of the CSA guidance and the new edition of the GAMP 5 guide, there is understandable apprehension and uncertainty. The ability to demonstrate control and satisfy the Four Cs, along with the ability to push a button and see an all-inclusive trace matrix with real-time data, will reassure stakeholders that the organization's risk management practices are solid. This is critical because a trace matrix is an excellent tool used by auditors to assess system validation.

> A trace matrix is the mortar that holds the validation bricks together; it should be used throughout the validation lifecycle.

Agile Validation

ValGenesis technology is a boon for significantly shortened validation and "fit for use" certification. It mirrors the Agile software development process. Software modules developed using the Agile framework cannot be certified as "fit for use" until (and unless) they are validated. This technology provides controlled flexibility for software module development and simultaneous validation. In addition to a controlled framework, ValGenesis also enforces a disciplined, compliance-driven software design and development process (technical controls, as mentioned earlier) and a change management framework to accommodate future system development iterations.

Scope Changes and User Stories

Scope changes precipitated by user story changes (aka user requirement changes) are easily addressed by the solution's ability to dynamically maintain the requirements to test traceability matrix. Subsequently, the design subject matter expert (SME) can select the user stories to include in the product backlog file. The backlog file cross-references the approved stories along with the corresponding acceptance criteria. Items chosen for sprints from the product backlog file trigger the development of the corresponding URS, FRS, test scripts, and other documents.

Figure 13 below demonstrates the seamless integration with Agile software development that ValGenesis technology provides. The screenshot displays the list of imported stories from software design documents.

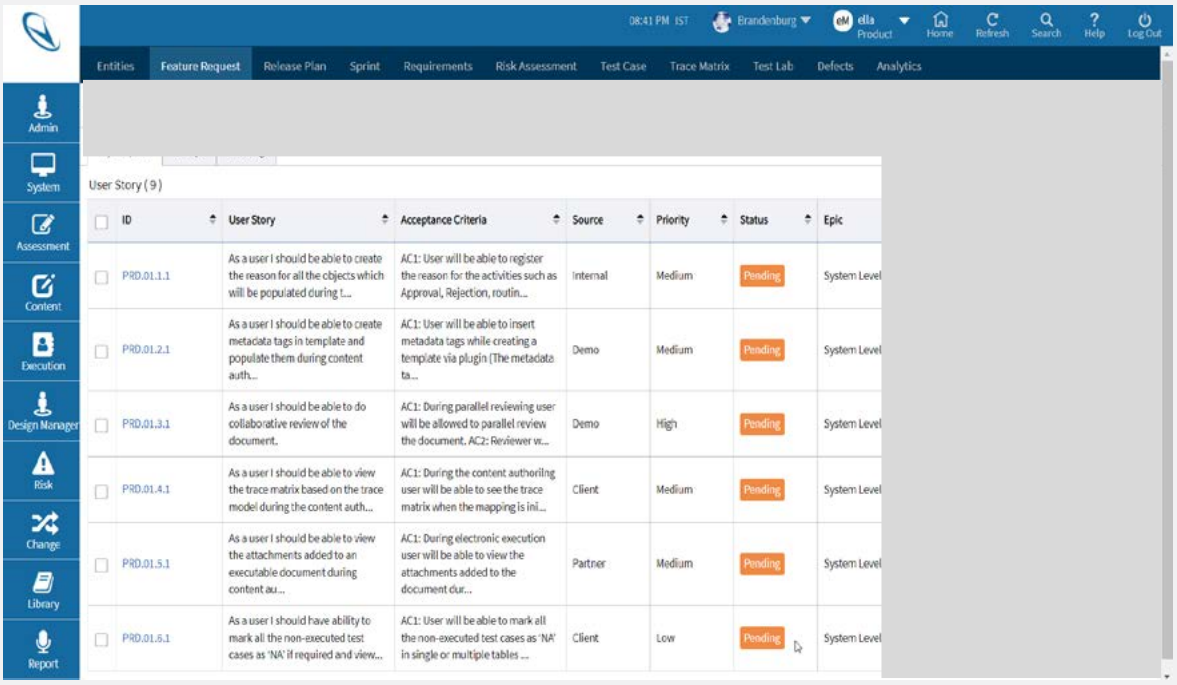

Figure 13. User Story Imports

Figure 14 below is a screenshot of the product backlog, which is a list of approved user stories.

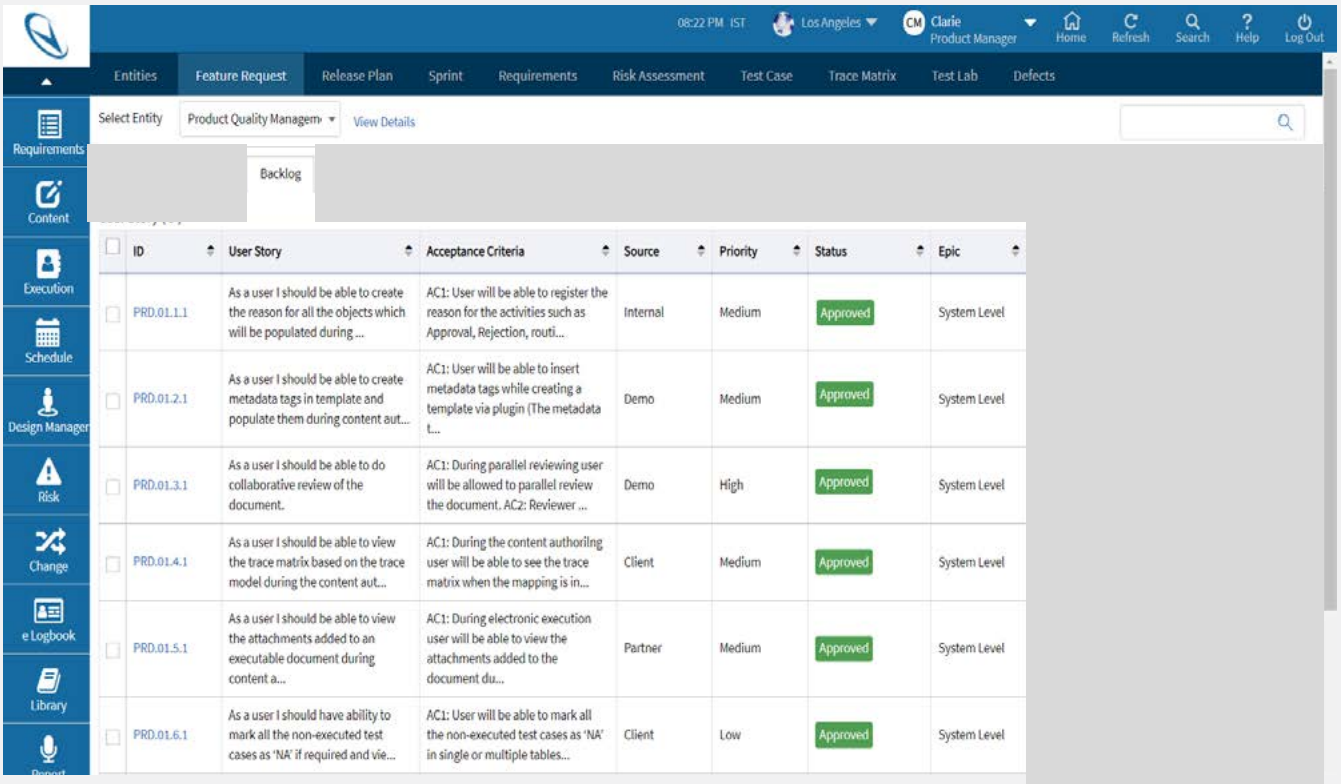

Figure 14. Product Backlog

Risk Rank to Determine CSA Test Category

After the URS and FRS for the sprint are approved, the system uses its internal messaging feature to route them to the risk assessment team. The assessment team assigns a risk rank for each requirement using a user-established scoring criteria. The system uses the risk rank to determine the CSA test category as specified in Appendix D5 of GAMP 5 E2. Figure 15 below is a screenshot of a typical risk assessment.

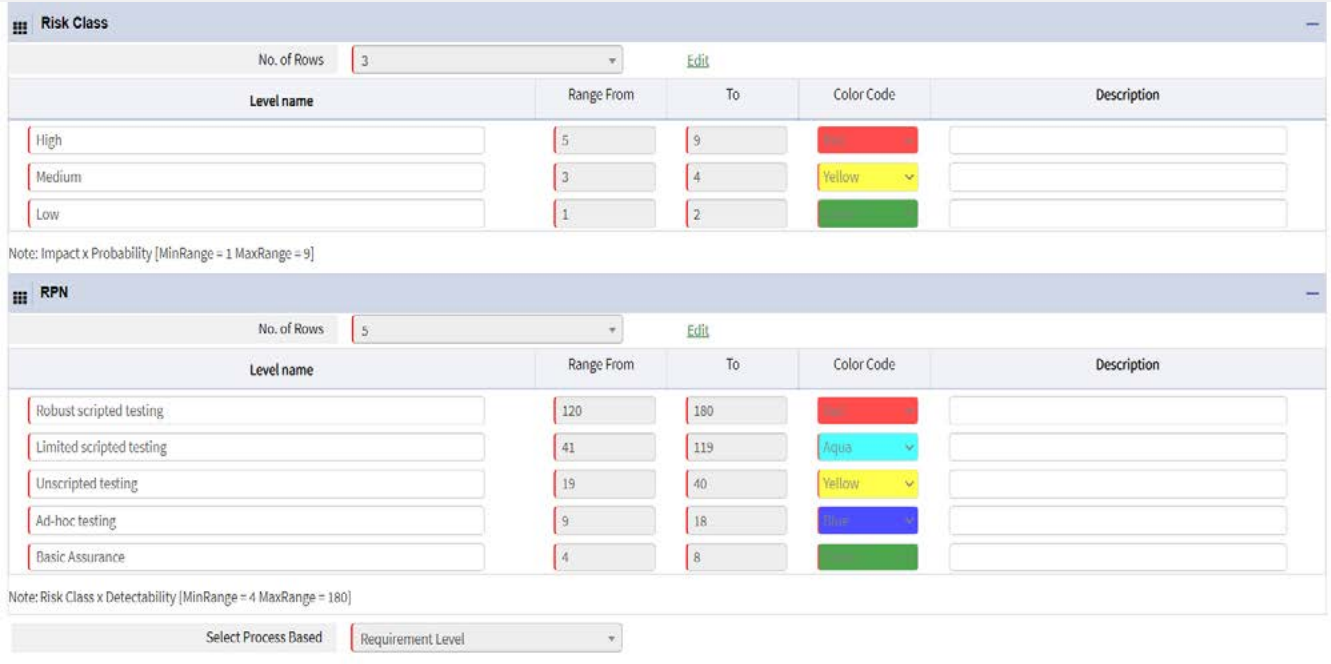

Figure 15. User-Defined Risk Priority Number (RPN) Scoring Criteria for a Requirement

ValGenesis Technology Salient Features and Benefits Recap

Supports ALCOA+ Principles

The diagram below (Figure 16) is a validation business process swim lane. Features introduced in the latest version of the VLMS are associated with tasks displaying red borders. These features enable Agile software validation activities to run parallel with Agile software development. They also provide an integrated environment for risk-based validation wherein risk assessment outcomes seamlessly enable the test categorization of CSA.

Once categorized, ValGenesis routes assigned test categories to the designated test developers to develop test scripts in user-predefined test forms. The consistency in risk scoring, test categorization, and test script development using standardized forms fulfills the data integrity requirements of the consistency principle of ALCOA+. The automatic routing feature of ValGenesis also removes the human element, which is critical for reducing data integrity issues.

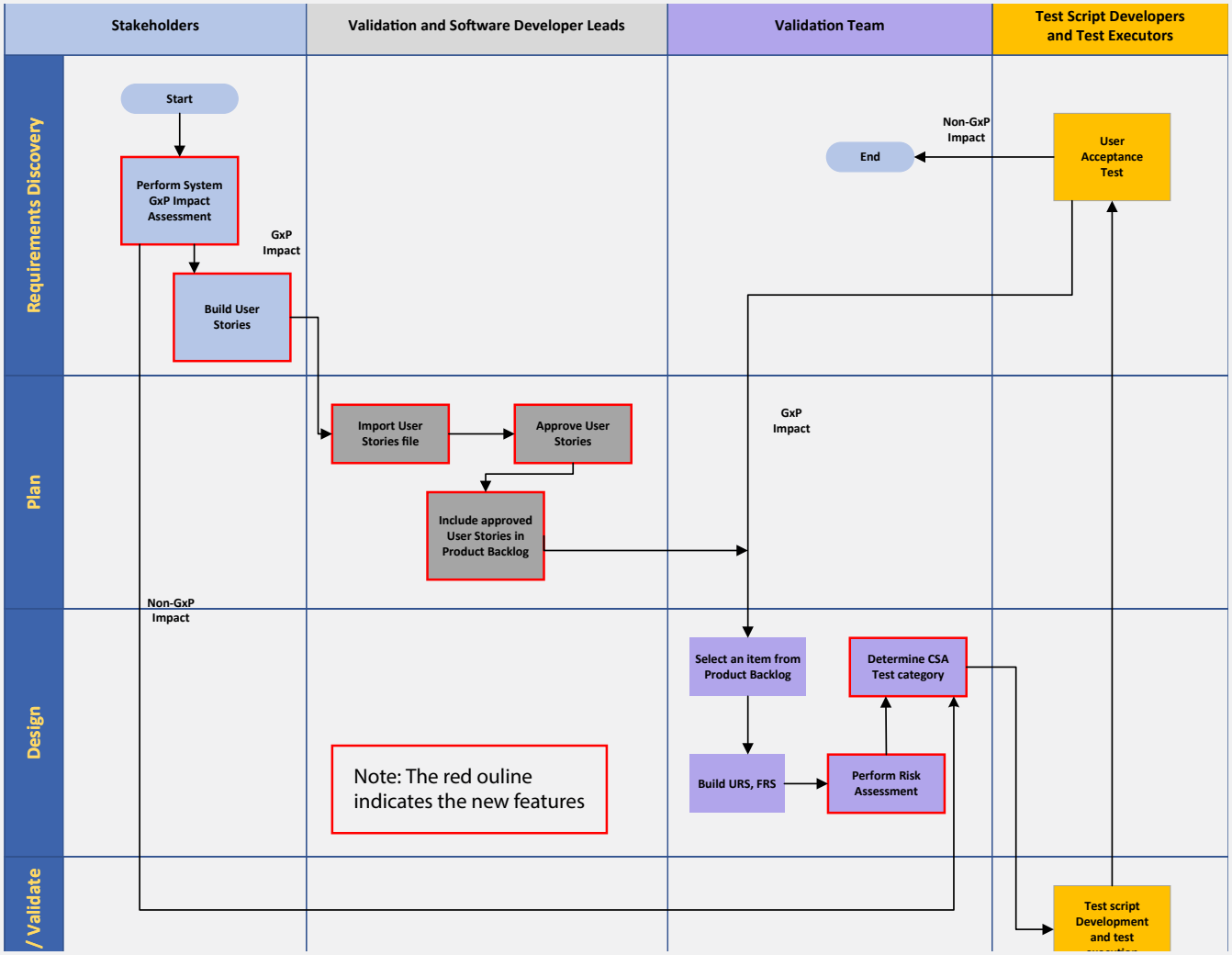

Figure 16. Example Validation Business Process Swim Lane

Validated Systems Repository

ValGenesis serves as a repository for all validated systems across the enterprise and makes them available on demand to regulatory authorities. The user can drill down to real-time validation details for the entire system in just a few clicks, as depicted in Figures 17 and 18 below.

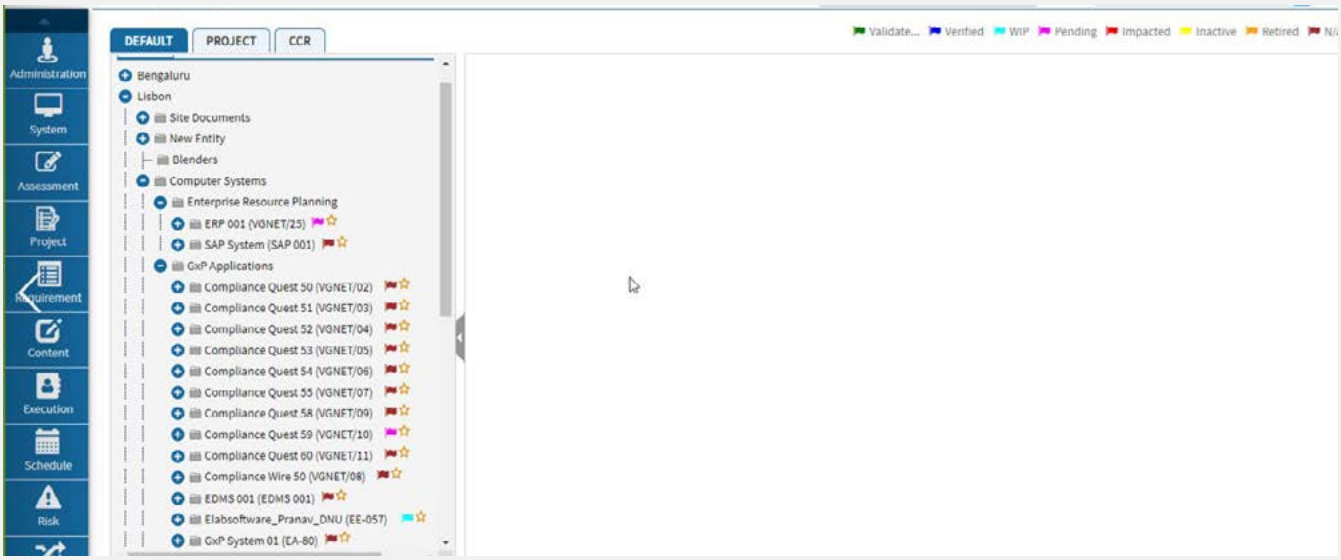

Figure 17. Validated Systems Repository

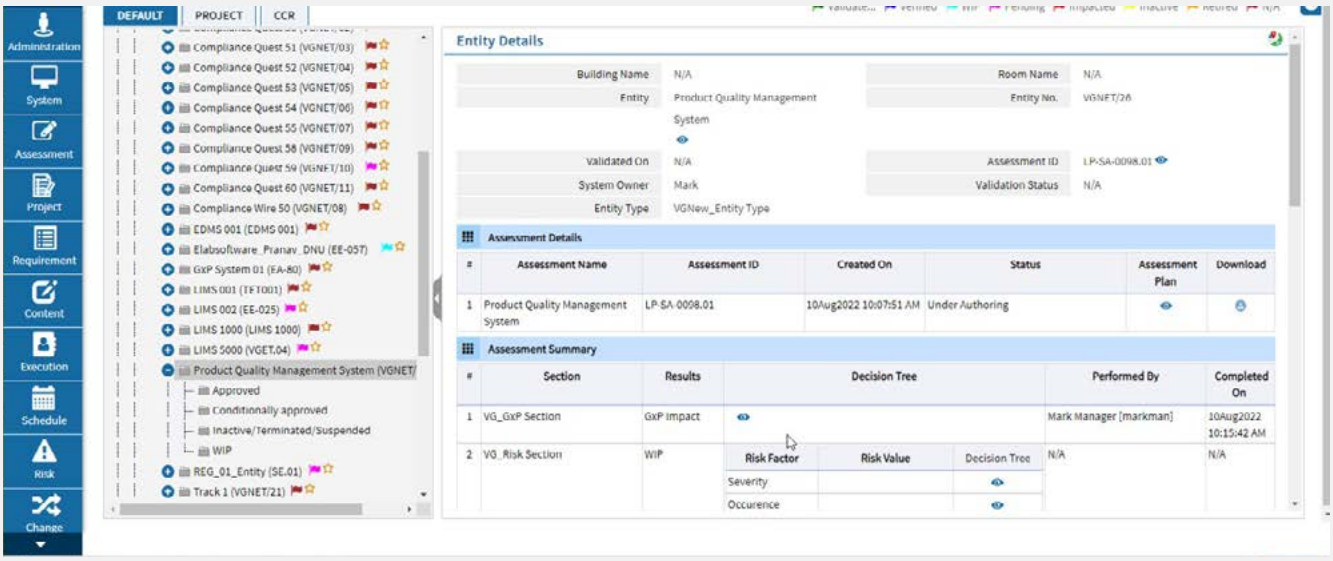

Figure 18. Validated Systems Repository

The on-demand feature fulfills the available principle of ALCOA+. It satisfies regulatory guidance that requires users to have an inventory of all validated systems (reference PIC/S Guidance PI 041-1 titled “Good Practices for Data Management and Integrity in Regulated GMP/GDP Environments section 9.2”).

GxP Impact Assessment

GAMP 5 E2 recommends applying critical thinking throughout the validation lifecycle. As a first step, a GxP impact assessment should be performed, followed by a detailed functional risk assessment (FRA). Using ValGenesis' Part 11-compliant role-based access feature, an authorized user can create the GxP impact assessment template and the relevant questions. Once approved, the template is locked to prevent unauthorized changes. It then becomes a standardized template for assessing GxP impact for all systems across the enterprise, fulfilling the ALCOA+ attribute of consistency. Figure 19 below is a screenshot of a typical GxP impact assessment.

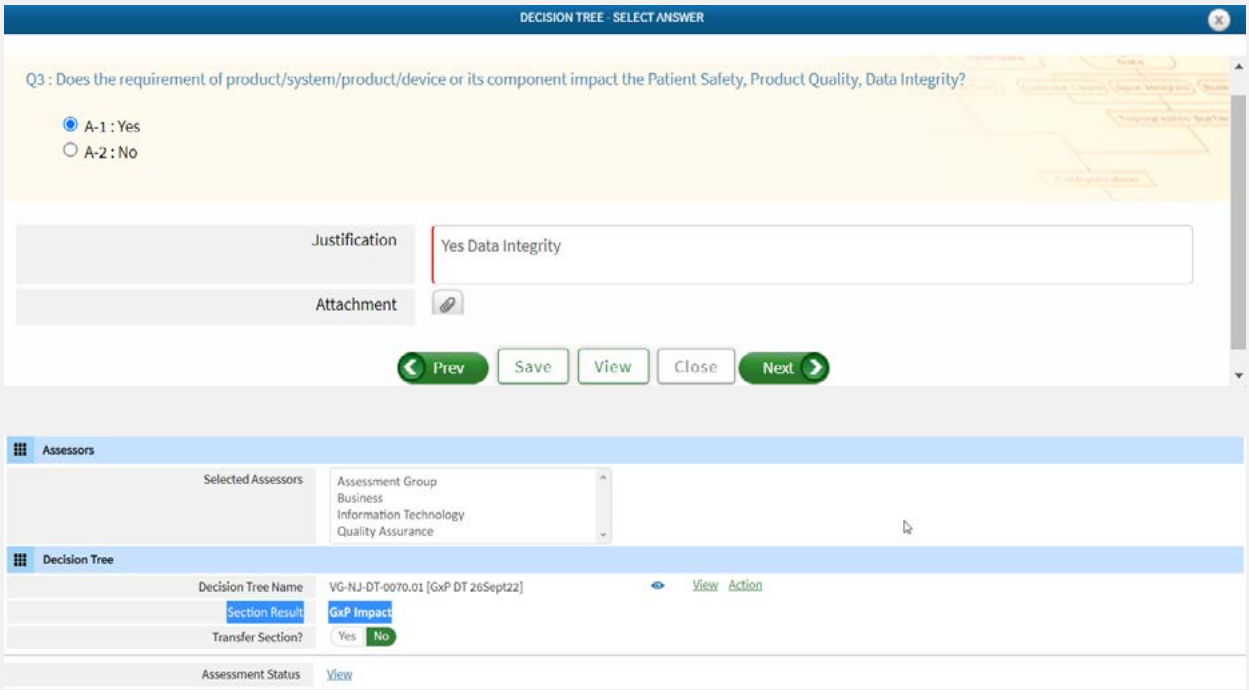

Figure 19. GxP Impact Assessment

A POWERFUL SOLUTION

By leveraging a technological solution like Design Manager, regulated organizations can:

- *Tailor custom risk models to meet various needs*
- *Drive consistency with technical controls*
- *Eliminate subjectivity by enforcing multi-factor matrices*
- *Support any risk model (FMEA, RPI, custom)*
- *Address all risk areas that impact patient safety and product quality*
- *Manage risk throughout the life of a system*
- *Automate traceability from requirement, through risk, to testing and controls*
- *Automate testing*
- *Identify impact of change automatically*
- *Automate reporting*

CONCLUSION

Digital technology is transforming the way life sciences operate, and the adoption of robust digital tools has become essential for survival in today's rapidly evolving market.

The ValGenesis VLMS is a modern solution that's purpose-built, risk-based, and data-driven. It meets and exceeds the functional requirements needed to help life sciences companies comply with GAMP 5 E2 and supports the testing strategies championed by CSA.

Powered by new Designer Manager technology, the system not only "rightsizes" the validation effort but also offers the maximum benefits of Agile software development, critical thinking, and smart validation. It provides a truly paperless, error-reducing system for addressing requirements scope creep, and other issues characteristic of cutting-edge manufacturing processes.

ValGenesis, Inc. is the creator of an innovative software platform that serves as a foundation for managing compliance-based validation activities in life science companies. ValGenesis, Inc. is the provider of the first enterprise application that manages the corporate validation lifecycle process. This solution is fully compliant with U.S. FDA 21 CFR Part 11 and Annex 11 requirements. As the first fully paperless solution for electronic management of validation execution and approval, ValGenesis was selected by an industry peer review committee to receive the Parenteral Drug Association (PDA) New Innovative Technology Award in 2005.

VALGENESIS®

www.valgenesis.com