Received: 11 May 2022 | Revised: 17 June 2022 | Accepted: 21 June 2022

DOI: 10.1111/vox.13332

Vox Sanguinis ISBT International Society of Blood Transfusion

GUIDELINES

International Society for Blood Transfusion Guidelines for Validation of Automated Systems in Blood Establishments

Jan-Willem Andriessen[1] | Michael Breard[2] | Lynne Briggs[3] | Suzanne Butch[4] | Patricia Distler | Jørgen Georgsen[5] | Shankar Goudar[6] | Teemu Laakso[7] | Robin Nozick

[1]Sanquin Bloedvoorziening, Amsterdam, The Netherlands

[2]Common $ense Consulting LLC NM, Las Cruces, New Mexico, USA

[3]Versiti, Milwaukee, Wisconsin, USA

[4]Michigan Medicine, Ann Arbor, Michigan, USA

[5]Department of Clinical Immunology, Odense University Hospital, Odense C, Denmark

[6]Carter Blood Care, Bedford, Texas, USA

[7]Finnish Medicines Agency Fimea, Helsinki, Finland

Correspondence
Jan-Willem Andriessen, Plesmanlaan 125, Amsterdam 1066CX, The Netherlands.
Email: jw.andriessen@sanquin.nl

Keywords: application validation, assessment, GMP, infrastructure qualification, IT security, risk, supplier qualification

Contents

This document has been written by the International Society of Blood Transfusion's Working Party on Information Technology, Validation Task Force.

INTRODUCTION

The objective of validation of applications and qualification of infrastructure is to produce documented evidence that provides a high level of assurance that all parts related to the use of an automated system will work correctly and consistently. There are many ways this objective may be achieved by a blood establishment. Given the complexities and critical control functions of today's automated systems, it becomes particularly challenging to ensure thorough, but not excessive, validation/qualification practices.

Once a validated/qualified automated system is in use, it is essential to maintain the validated state by periodically testing and reviewing its performance.

These guidelines, produced by the ISBT Working Party on Information Technology (WPIT) provide insight into the development of appropriate practices in these areas. They were originally published in 2003 and again in 2010. While many concepts of validation have remained the same, the ISBT WPIT has updated the guidelines and expanded them in the following areas:

- infrastructure qualification;
- supplier qualification;
- qualification of virtual computerized systems;
- disaster recovery planning;
- periodic review;
- software patches/service pack installation and
- backup and recovery.

These guidelines do not advocate a particular validation/qualification methodology but do promote the Quality Risk Management approach advocated by GAMP® 5 [1–3] and ICH Q9 [4], a life cycle approach within the QMS and the use of risk assessments to define the validation/qualification strategy for critical systems. They are intended to be relevant and applicable to all blood establishments regardless of the approach adopted by each or the level of development and resources. To adapt the guidelines to an organization's needs and to be compatible with existing programmes such as the Africa Society for Blood Transfusion (AfSBT) Step Wise Accreditation Programmes (SWAP), consideration should be given to:

- the size and type of the organization;
- the probability and impact of risk to the organization;
- the diversity of activities taking place in the blood establishment;
- the dependence on the automated system for critical control and blood product quality;
- applicable regulations and standards;
- opportunities to leverage the supplier documentation and knowledge and
- the availability of needed resources.

Finally, the approach to validation/qualification used by a blood establishment must allow for the process to be scalable to the functionality of the system, for example, the validation of a centrifuge is less complex than that for a bespoke blood management system.

The WPIT, therefore, encourages each blood establishment to determine for itself appropriate policies and practices for the validation and maintenance of the validated state of its automated systems using these guidelines as a reference.

OVERVIEW

Every blood banking organization must have a Quality Management System (QMS). It is the management's responsibility to participate and approve sign off on the design, implementation, monitoring and maintenance of an effective QMS. It should include a section on validation (e.g., Validation Master Plan or Validation Policy) that describes the organization's policy regarding the validation of equipment, facilities, utilities, methods, processes and automated systems required during the procurement, production and use of blood components. An organization's validation policy should comply with the regulatory requirements applicable in the country of use.

The guidelines are not intended to present a new concept of validation but to be relevant and applicable to all blood establishments regardless of the approach to validation adopted by each. They were originally built upon other field validation experiences and have been updated with the experience gained in validating automated systems in blood establishments.

The benefits of validation are that it:

- improves the use of technology;
- increases the business benefits of computerized systems;

- improves the relationship between stakeholders (users, suppliers, authorities, etc.);
- improves operational efficiency;
- reduces the risk of failure and
- improves compliance with regulations.

These guidelines address the validation needs for automated systems, that is, those that have some degree of computer control. The use of a project process methodology facilitates the achievement of validation requirements and provides the necessary level of control.

Testing of software is not in itself 'validation'; it is a verification activity. It should not be separated from the overall validation of a process/system.

Validation is more than simply testing an application, process or system. Its objectives are:

- to demonstrate control;
- to ensure compliance;
- to generate knowledge and
- to establish future requirements (e.g., training and maintenance).

Validation requires a structured approach. The approach normally used for automated systems makes use of the concept of a computer system life cycle. Approaches may include methodologies developed initially to manage software development and medical device verification. Approaches such as agile validation may be used as long as there is adequate documentation of work performed.

A computerized system life cycle includes phases from the initial concept of the system, through project and operation phases, and through the retirement of the system. The activities of these phases are systematically defined when adopting a life cycle approach within the QMS. The life cycle activities should be scaled depending on the outcome of a risk assessment, systems components, supplier capability and business impact. The life cycle approach enables management control and a consistent approach across systems. It ensures compliance with regulatory requirements and assurance of quality and fitness for the intended use.

Determining what to validate

Blood establishments have to validate all automated systems and computer systems that are considered critical. The system is considered critical if:

- The automated system is directly linked to the decision-making process for blood or blood product manufacturing, testing (donor/patient), labelling and release for transfusion and/or it is used to manipulate the related information.
- The computer system is critical to product and quality, information management, record storage, and tools for operational decision-making and control.

The objective is to produce documented evidence that provides a high level of assurance that all parts related to the use of an automated system will work correctly and consistently.

Deciding how much validation is enough

A question often posed by blood establishments is: How much validation do we need to perform?

Validation is essentially a component of the organization's quality management system, so this question could be rephrased as 'How much quality do we need?' The product quality and cost benefits to be achieved by an organization through adopting the Total Quality Management principles of customer satisfaction, employee involvement and continuous improvement are well-established and are equally applicable to validation.

The answer to the question, therefore, is that the blood establishment needs to ensure that enough of the right work is done by the right people to achieve system acceptance in a way that satisfies the Quality System.

With this in mind, it is worth considering what makes validation projects successful, namely:

- senior management commitment;
- sufficient resources;
- competent project management;
- collaborative team approach, that is, users/technical representatives/validation/quality assurance (QA)/Information Technology (IT) professionals;
- risk assessment and
- cost efficiency.

Validation is a complex process. The skill sets and experience of the team are very important in ascertaining the scope of work to be carried out and that not too much or unnecessary work is performed. There may be a temptation to disregard particular elements to reduce workload. This approach is not recommended and should be avoided.

Determining the resources needed

The process is easier to perform with qualified staff and where validation processes are already established and embedded into the organization. For those organizations that are about to adopt validation practices and that may be lacking validation resources, it is important to consider the following:

- It takes time for validation processes to be developed and become embedded in the organization. In the meantime, the blood establishment wants to continue with its activities.
- It is essential that validation and acceptance of systems are performed before systems are used operationally.
- Use should be made, where possible, of the supplier's system and test documentation to reduce the blood establishment's qualification effort.

PURPOSE

These guidelines were first developed and have been updated by the Validation Task Force of the International Society of Blood Transfusion Working Party on Information Technology (ISBT WPIT).

The aim of these guidelines is to provide guidance on the validation of automated systems in blood establishments which may affect the safety and quality of blood components and services provided by organizations involved in blood collection, testing, processing, distribution and/or transfusion.

Technology is rapidly advancing. These guidelines should serve as a basis for validating emerging as well as existing automated systems.

SCOPE

This document addresses related activities such as application validation, supplier qualification, risk assessment, data migration, disaster recovery planning and IT-specific topics.

- This document does not cover steps in the validation of interfaced automated equipment.
- This document does not cover national regulations.

RESPONSIBILITY

The overall responsibility for ensuring that all critical automated systems are validated lies with senior management.

The validation team may include validation specialists, quality assurance staff, operational users, information technology staff, engineering staff, suppliers, purchasing staff and consultants. The minimum membership of a validation team should be representatives of the process owner, IT and quality assurance. The actual membership will be determined by the scope of the validation. Within certain constraints (e.g., personnel reviewing the validation should not have executed the tests they review), individuals on the validation team may have multiple responsibilities. All validation activities must be communicated to or even involve the top management of the blood establishment.

The following are examples of responsibilities that may need to be assigned to members of the validation team:

- management of the validation process;
- quality assessments of third-party suppliers;
- preparation, execution, review and approval of validation plan and protocols;
- problem resolution;
- identification of required materials and support;
- filing and maintenance of all completed validation documentation;
- verification of data migration;
- development of documents, including Standard Operating Procedures (SOPs) and
- preparation, execution, review and approval of training plans.

CHANGE CONTROL

Any change occurring during a project (before releasing an automated system) or to an operational automated system should be documented in order to ensure that the system is maintained in a state of control.

Change may be initiated by the process owner or others, but it should be controlled by the process owner.

Project change control

During the validation process, before releasing an automated system for operational use, modifications to the configuration of the automated system may be made to comply with specifications and/or end user expectations.

Any change occurring during the validation process must be documented and controlled.

All deliverables in the context of the project or system should be identified, so the items subject to change control may be defined. These include:

- IT Infrastructure;
- hardware;
- software: including application software, operating systems, Database Management Systems (DBMS); firmware, library files, configurable packages, drivers and compilers;
- configuration files/reference tables;
- data migration files and programmes;
- manuals (user manuals, system manuals);
- development documentation;
- validation documentation;
- training materials and
- Standard Operating Procedures (SOPs).

Modifications to system configuration and/or validation deliverables resulting from test deviations encountered during the qualification phases are subject to project change control.

Operational change control

Changes to a live, automated system are managed through the facility's change management procedure. Some changes may require notification to or license amendment from regulatory agencies. Since this varies among countries, users must consult local requirements. Operational change management should continue until system retirement.

All proposed modifications, enhancements or additions should be reviewed and assessed to determine the effect each change would have on the system. This operation should determine the degree of required validation. When changes are made to an automated system, sufficient validation should be conducted to demonstrate that portions of the IT infrastructure and software not involved in the change were not adversely impacted. This is in addition to testing that evaluates the correctness of the implemented change(s). Where required, SOPs and Configuration Management Database (CMDB) should be updated and user training updated and delivered before implementing the changes. All other relevant documentation should also be updated.

Operational change control SOPs should allow for specific variation for certain types of changes such as system administration

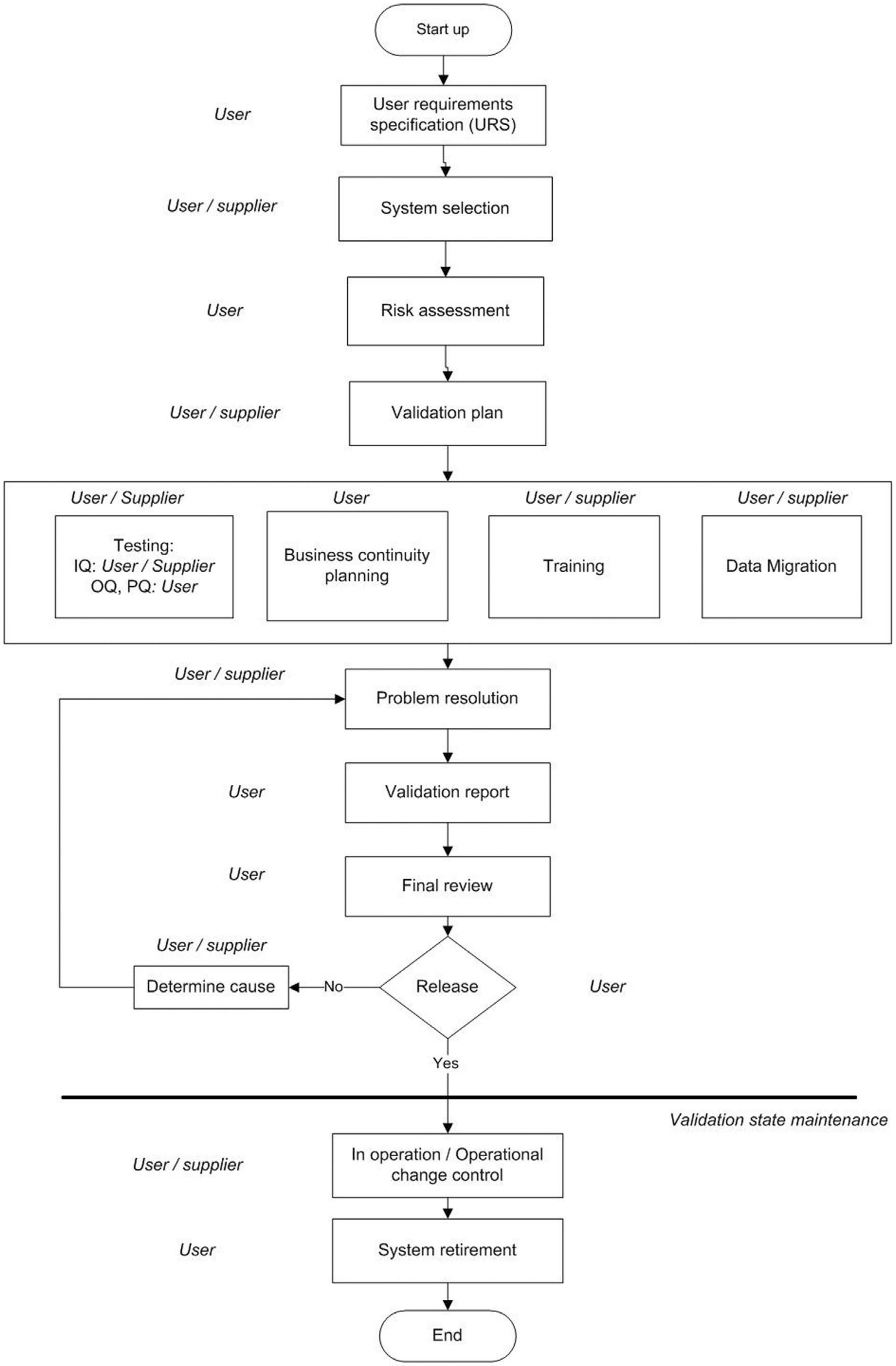

FIGURE 1 Validation process throughout automated system life cycle

Responsibility of the user and supplier is attributed for each step of the validation process modifications, emergency or repair changes or for workarounds provided by the software vendor.

It is the responsibility of

- the system process owner to ensure that a change control process and associated procedures are in place to support changes to the system;
- the management team to ensure SOPs are followed and
- each member of the change team to execute the assigned activities accurately and completely.

Just as in the guideline sections above, operational changes require a well-thought-out, defined and documented change management plan and process – whether for planned or unplanned changes. This process assures that the system remains in a state of control or can be returned to the previous state of control and is authorized by the appropriate personnel as defined in the facilities plan.

At a minimum, an infrastructure change management plan should consider the complexity and impact of the change and include the following:

- defined change control team
  - quality staff;
  - IT personnel appropriate to the change;
  - review/advisory panel knowledgeable in the system;
  - stakeholders (others impacted by the change) and
  - final authority;
- request – a defined and controlled method to request a change to the infrastructure, including a description of the change, scope and proposed timeline;
- risk and impact analysis;
- consideration of human and financial resources;
- justification – specific outcomes and impact on business, technical and other systems/services, including a risk analysis of these systems;
- test and validation plan – defined testing requirements, at what stage(s), validation requirements, who is responsible and who signs off – the amount of detail will depend on the complexity and the impact of the change;
- backout plan – how to return the system to a state of control if there is a problem either during the change or after the change is implemented;
- implementation plan – including a timeline, resources required and any training/competency required in a manner that will minimize disruption to end users;
- post-implementation review/lessons learned – to assure that the change is working as planned and has not created problems and
- final change review and documented acceptance – a review of all aspects of the change and sign-off by the appropriate individuals as identified in the change management policy.

In an electronically connected world, there are attacks on entities through the Internet. Therefore, it is critical to accept some changes to a system, such as a security patch after a breach. Sometimes a change to the system is less risky than not making the change or waiting until after the completion of testing before making the change. There should be documentation which details why the critical safety patch was needed and that it was installed. It is necessary to test the system to ensure critical functionalities of the system are not affected. In these cases, it is also important to monitor the system closely after installing a critical safety patch to ensure there is no unintentional negative impact of the patch.

Because critical safety patches may be installed without verification, suppliers that provide these services should also follow good IT practices, including quality planning which defines the activities, procedures, deliverables and responsibilities for delivering and monitoring their services.

System inventory

An up-to-date listing (inventory) of all relevant systems and their GMP functionality should be available.

It should consist of:

- name of the system;
- version or model number of the system;
- the owner of the system and
- its validation status.

For critical systems, an up-to-date system description detailing the physical and logical arrangements, data flows and interfaces with other systems or processes, any hardware and software prerequisites and security measures should be available. For this purpose, a CMDB can be used.

VALIDATION PROCESS THROUGHOUT THE AUTOMATED SYSTEM LIFECYCLE

Figure 1 outlines the validation process.

Start-up of validation

Validation should start when the decision is made to acquire a new automated system (including a new information system or new equipment) or to implement a new process. Change to an existing process should also initiate validation as part of the change control procedure. This first step requires the identification of the stakeholders involved.

User requirements specification

An automated system is validated against its User Requirements Specification (URS). The URS is a key document that describes what the process owner wants or expects from the system. It is required for a new automated system or significant change to an existing system (minor changes should be captured by the change control process), whereas it does not include any 'how', it should clearly state what is required. The URS should form the basis of the contract with the supplier providing additional documentation and system definitions to support the procurement process.

The development of a URS is not an easy task and requires both expert knowledge of the business and analytical skills. It is the user's responsibility but often may only be completed following consultation with potential suppliers or independent experts. The approval of the URS should be documented in accordance with the facility's QMS followed.

In the case of custom-developed software, the URS will form the basis for a Functional Specification (FS), which describes each of the system functions necessary to meet the user requirements. Within the URS, use cases can be used to provide more detail.

GAMP® recommends the following during the production of the specification:

- each requirement statement should be uniquely referenced and be no longer than 250 words;
- requirement statements should not be duplicated or contradicted;
- the URS should express requirements and not design solutions;
- each requirement should be testable and traceable;
- both user and supplier need to understand the URS; ambiguity and jargon should be avoided;
- wherever possible, the URS should distinguish between mandatory/regulatory requirements and desirable features;
- GMP requirements regarding the supplier's quality system should be included;
- in the case of cloud service providers, the supplier will support the facility during the validation process by leveraging validation documents, and
- information security requirements should be included.

System selection

System selection is based on the following considerations covering the entire life-cycle of the system.

URS review

The URS is sent to potential suppliers as a request for a proposal. A supplier's response should be based on the functionality of their system (functional and technical specification) and how well they meet the user requirements. During the URS review, the responses of the supplier candidates and/or their system FSs are compared with the URS in order to identify suppliers and systems that may qualify.

Supplier qualification

An important part of the validation, which is not a testing activity but is vital to the quality of blood and blood components, is assessing a supplier's ability to provide critical components of computerized systems [including a Blood Establishment Computer System (BECS)], whether hardware, infrastructure, cloud services or software.

Purchasers must ensure that suppliers have implemented QMS. Suppliers of BECS must follow the Quality System Requirements in the country where the BECS will be installed. Since suppliers of BECS may install their systems in multiple countries, harmonization of their Quality Systems used across the world has become best practice. There should be a methodology in place to verify the suitability of suppliers of BECS, critical IT equipment and services prior to selection.

A Computerized System has been defined in GAMP 5 [3] as: "Any automated or digital system used in the business. The Computerized System consists of the hardware, software and network components, together with the controlled functions and associated documentation."

The supplier of critical IT products and services should be assessed using a questionnaire/survey, an on-site audit or a combination of both. A qualified auditor or a third party can also perform the audit of the supplier if needed.

The assessment should evaluate the status of the supplier's quality system. Attention should be given to the supplier's procedures for the development, support, maintenance and distribution of updates. If the supplier is an existing supplier, the results of previous assessments should be reviewed and taken into account when evaluating the supplier. Arrangements for the supplier assessment should be formally agreed upon by the user and supplier and documented.

Supplier qualifications such as ISO 9001 and 27001 can be taken into consideration when qualifying a supplier.

For less critical services and products and for suppliers of infrastructure and professional services, assessment by questionnaire is sufficient.

The use of referrals and information found on the Internet about the service-oriented company may be as useful as an audit to verify the company's adherence to their QMS and how successful it is at adhering to requirements and delivering its services to clients. However, it is recommended that a combination of both methods (audit plus Internet search) be used. If possible, find another blood establishment that used the service company for a similar service and ask probing questions to uncover any non-adherence to cGMPs.

Supplier qualification may vary depending on the type of service provided. For example,

- For an infrastructure or platform supplier, infrastructure life cycle, security control/measure implementation, continuity of infrastructure and availability of installation documentation should be assessed.
- For a software provider, the existence of a software life cycle, change control policies, data integrity, user documentation, control of user access and availability of validation plans for software should be assessed.

Each potential BECs supplier's QMS should include a documented policy to ensure that the automated systems introduced to blood establishments are compliant with GMPs and adequate for the systems' intended use.

The supplier's QMS should:

- integrate life cycle activities for the process being followed to deliver and support the product, application or service;
- specify responsibilities, including making it clear there should be a separation of authority between quality assurance and other groups, such as product development, product support, finance or marketing;
- determine the appropriate deliverables, documentation and planned periodic reviews of supplier's adherence to the QMS;
- follow a validation framework, including the use of validation plans and validation reports as necessary and
- maintain compliance throughout the life of a system and have an approach to continuous improvement of the QMS and its use.

Some potential questions that can be used to ascertain a supplier's suitability for activities, services or supplies as part of a medical device may be found in Appendix A.

System evaluation

System evaluation consists of assessing:

- the system against regulations and standards, including GxP;
- the system against established user requirements;
- the needs of the system and environment configuration;
- the requirements for installation;
- the training requirements;
- the technological standard of the system, that is, future proofing and the road-map of the future development and
- the supplier to ensure it uses a recognized development methodology.

Evaluation will be against criteria specified by the user in the URS. Results of the system evaluation should be presented in a report.

From the user perspective, system evaluation should be performed on critical automated systems that are configurable, off-the-shelf packages or bespoke developments.

Financial considerations

Depending on national policies, financial consideration is an important element in the selection of a new automated system. The user should consider costs of the entire life-cycle of the system including:

- one-time implementation costs such as:
  - software licensing;
  - hardware, interfacing and peripheral costs;
  - data migration, installation and training costs;
  - validation effort needed and
  - travel and lodging expenses.
- on-going costs, such as:
  - software support;
  - hardware and network maintenance;
  - yearly fees for infrastructure and software licenses and/or service;
- archiving of historical data and records;
  - frequency of anticipated software updates and system upgrades and amount of revalidating involved;
  - additional staffing in technical, quality, end user areas, etc. and
  - retirement costs.

Risk assessment

Risk assessment is required when an automated system is new and to be implemented, changed, upgraded or its retirement planned. It must be performed to identify critical control points, determine the degree of testing required and define risk mitigation plans. This requires considerations of the impact, probability and detectability of a potential hazard or harm to a computerized system.

Risk assessment also looks at the critical control points in the software and can identify those areas where, if there is a failure or malfunction, harm to the patient, donor or business may occur. Risk assessment should at least consider the following elements: patient risk, product quality and data integrity.

A risk assessment has an important place in the validation process as it can maximize testing resources. Since it is impossible to test everything, it is best to identify the higher risk functionalities and spend proportionally more time and effort on validating these processes.

Many automated systems used in blood banking are considered to be configurable software packages. A typical feature of these systems is that they permit each institution to develop its own applications by customizing/configuring the system. Each application then becomes specific to this institution, and maintenance of the system becomes an important process, especially when new updates to the system are installed. Often, the configurable system is part of a much bigger network, which, in turn, becomes the entire system. This makes it impossible for the vendor to validate each different type of final system. The amount of testing and how many times the same process is tested is dependent on the amount of risk the functionality may present. This should provide the user with a higher degree of assurance that the system will consistently produce a quality product.

A systematic approach is needed to perform a thorough risk assessment. First, each potential risk of a system or subsystem is identified and traced to a trigger, event or cause. Information regarding each potential risk is collected, analysed and a GAMP [3] category assigned (see Appendix B). For an example of risk categorization see Table 1.

TABLE 1 Risk categorization

High	Risks are considered to be intolerable
Medium	Risks are undesirable
Low	Risks are so low as to be negligible

TABLE 2 Documentation important to the validation process

Steps of the validation process	Type of documents	Supplied by
User requirements specification	User requirements specification (URS)	User
System selection	Installation requirements *Functional specifications *Hardware design specifications *Software design specifications *Engineering diagrams Manual/user guides Supplier questionnaire/survey Supplier audit report system evaluation report change management policy	Supplier
Risk assessment	Risk analysis	User
Throughout	SOPs Use of the automated system Support activities Backup and recovery Archiving and record retention Change control Security management Periodic review Business continuity/disaster planning System retirement Training Maintenance and monitoring	User
Validation plan	Validation plan Validation protocol	User
Training	Training plan Documentation of training Training material	User and supplier
Testing (IQ)	Test results	User and supplier
Testing (OQ, PQ)	Test results	User and supplier
Disaster recovery plan	Countermeasures plans Disaster recovery plans Continuity action plans	User
Problem resolution	Problem resolution records	User
Validation report	Validation report	User
In operation	Maintenance and monitoring plans and records Periodic audit/review plans and reports Change control and incident records Data migration plan	User
	Change notification	Supplier
System retirement	System retirement plan and report	User

Note: *User may have to assume that supplier has these documents.

Next, options should be provided for risk reduction to either mitigate and/or eliminate the risk. It may be decided that the risks in the system are so high that it should not be implemented. If it is decided to go forward with implementation, controls, either process or product, need to be used to mitigate and/or eliminate the identified potential risks. Mitigation generally involves testing or creating workarounds, either with independent software or written SOPs that prevent the end user from replicating the risk identified in the system process. Documentation of the entire process must be produced, approved, controlled and retained for the period required by national regulations. Table 2 includes documents that are typically required to provide an audit trail and assure the quality of the validation process, including the maintenance of the validation state.

Validation plan

A validation plan should be prepared after a decision is made to implement a new or change an existing, system. It is recommended that the validation plan be prepared as a cooperative effort by subject matter experts, IT, quality and production management staff. The level of risk is a major factor in determining the level of effort to be applied in testing and other verification and validation tasks. It may be revised, under change control, during the life of the validation process. Once the validation is performed, the plan becomes a historical record.

The validation plan should provide a description of:

- the automated system;
- the validation activities;
- responsibilities;
- the procedures used during the validation;
- operating procedures post-implementation;
- expected outcomes and
- acceptance requirements.

User and supplier roles and responsibilities for validation activities must be defined. The identity of authors, reviewers and approvers of the deliverables must be identified in the plan. Procedures for documenting, reporting, evaluating and resolving incidents and deviations discovered during the validation process should be included, as well as a mechanism for documenting and justifying exceptions to these procedures and the validation plan.

The completed validation plan must be reviewed and approved according to the facility's quality system policies. The validation protocols are used to produce documented evidence that the system performs as intended.

Content of the validation plan

The validation plan should cover the following topics:

Scope of the validation. The scope of validation should specify the automated system's identification, the context of the use of the automated system, the automated system's definition, the automated system's boundaries, that is, what is in and out of scope for this validation project, the processes to be employed and the aim of the validation.

Risk management. Risk management should involve an initial assessment, including a decision on whether the system or its part(s) is GxP regulated or not.

Validation strategy. The strategy to follow for validation will depend on the type and complexity of the automated system and the degree of risks of its use. It is mainly based on the different elements identified in the risk assessment and documents provided by the supplier concerning the supplier testing performed, use and administration of the automated system. The amount, type and results of supplier testing may be used to focus on and determine the amount of testing needed during the validation efforts.

Validation strategy should define which activities may be performed *prospectively*, *retrospectively or concurrently* (see Glossary for definitions of validation, prospective; validation, retrospective and validation, concurrent). The strategy must define the system platform(s) and controlled environment upon which the qualification processes are to be performed. Qualification of complex blood management systems would ideally take place upon a frozen test system, which is identical to and separate from the live environment. Less complicated equipment should be isolated from the operational environment during the validation testing. Installation Qualification (IQ), Operational Qualification (OQ) and Performance Qualification (PQ) classify the different validation tasks and testing that have to be performed to ensure the quality of the use of an automated system.

Installation qualification (IQ). IQ shows that the system has been installed correctly. Once IQ has commenced, the system and infrastructure should be under formal change control. Support from the supplier is required during IQ testing. Important IQ considerations are:

- hardware and software installation;
- installation conditions [wiring, utilities, uninterrupted power source (UPS) etc.];
- interface connections exist;
- preventative maintenance;
- safety features;
- supplier documentation, prints, drawings and manuals;
- software and hardware documentation;
- spare parts list;
- software backup;
- security aspects and
- environmental conditions (such as temperature and humidity).

Operational qualification (OQ). In this phase, the automated system and process operating parameters should be challenged to ensure that they will result in a product that meets all defined user requirements under all anticipated conditions of manufacturing, including worst-case testing.

OQ considerations include:

- functionality of the automated system;
- alarms and limits;
- configuration;
- process control limits monitored by the automated system;
- software operational parameters (ideally linked to the functional and design specifications as provided by supplier);
- automated system operational specifications;
- interface testing;
- process operating procedures;
- process change control;
- training;
- preventive maintenance and monitoring;
- evaluations for potential failure modes and worst-case conditions (risk analysis and critical control points, failure mode and effect analysis, fault tree analysis);
- backup and recovery and
- system access and security.

Performance qualification (PQ). The objective is to demonstrate that the computerized process will consistently produce acceptable product/output under normal operating conditions. Due to practical reasons, part of the limiting and boundary conditions testing is often performed at this stage. The demonstration is achieved by using the appropriate methods and tools for process validation.

PQ considerations include:

- use of actual computerized parameters and procedures established in OQ and used during the operation;
- reconfirmation of acceptability of the computerized processes as established in OQ;
- reconfirmation of process repeatability and assurance of process stability when used in the field with trained operators;
- data migration to the new platform and
- stress or load testing (data to prove stability and capability of the automated system).

Challenges to the process should simulate conditions that will be encountered during the operation. Challenges should include the ranges of conditions covered by the SOPs and should be repeated enough times to assure that the results are meaningful and consistent. Challenges will need to include forcing the process to operate at its allowed upper and lower limits.

Reports of qualification activities should be written and adherence to the requirements documented. The qualified infrastructure should be under change control.

Supplementary qualification(s). For more complex systems, it is often necessary to expand the qualification exercise to include functionally specific testing, which does not readily conform to the criteria for IQ/OQ/PQ defined above. For example, a separate Interface Qualification may be required when validating interconnected systems or a Cutover Qualification may be required to verify system security or operational features following the installation of the system in the live environment.

Formation of the validation team. The use of a team ensures that the validation processes are well analysed that the protocols are comprehensive and that the final validation package is well documented and easy to follow. The team should advise about 'worst-case' scenarios, communicate with key functional areas about new and changed products and foster cross-functional cooperation. Members of the validation team include end users, quality assurance staff, IT staff and others (facilities engineering, manufacturing, laboratory, technical services, research and development, regulatory affairs, purchasing and top management) depending on the subject.

Timeline. Depending on the complexity of the validation process, a timeline should be established in order to:

- evaluate the time and resources needed for the validation;
- define the period over which the validation should be performed and
- define the time when the automated system should be operational.

Validation deliverables. Relevant documents that must be obtained during the testing process should be specified (screen prints, installation reports, SOPs that have to be produced, graphical displays, electronic data, etc.). These documents will be used to evaluate whether the automated system can or cannot be released.

Acceptance criteria. The general acceptance criteria for validation testing and the acceptable overall outcome of the validation process should be defined in the validation plan.

Responsibilities and approvals. The plan should identify roles and responsibilities, as well as the individual(s) responsible for approval for release into production.

Validation protocols

Validation testing is performed using detailed validation protocols, which are developed as required from the validation plan and the risk assessment. For IQ, OQ and PQ, validation protocols should contain:

- the scope covered;
- the test instructions;
- the expected results;
- the acceptance/rejection criteria;
- spaces for capturing results of the tests, including a pass or fail statement that confirms the outcome of the test and
- a section for the tester and the reviewer to sign and date.

Validation protocols should be independently reviewed upon completion.

Data migration

Data migration is the process of transferring existing data, either manually or electronically, from a source system to a target system (usually from an old system to a new system). The source, as well as the target, can be single or multiple systems. Data migration may vary in scope, complexity and risk. The data migration process should be managed according to a specific plan and requirements described in a data migration plan. The goal of a data migration validation is to ensure data integrity in the new system(s).

The content of the data migration plan may vary depending on the complexity of the data migration processes. It must set forward sufficient elements to guide the data conversion team to a successful data migration. The plan should cover:

- migration scope;
- roles and responsibilities;
- requirements and deliverables;
- risk analysis;
- configuration management strategy;
- software tools and strategies for ensuring compliance and fitness for the intended use;
- data quality assessment;
- data mapping;
- data cleansing rationale;
- data transformation rules;
- migration steps;

- data verification strategy and acceptance criteria;
- system transition plan and
- rollback or workaround strategy if the migration fails.

Plan

In the planning stage, the first step is to perform a general assessment of the requirements. Based on a risk assessment approach it is essential to identify and develop key elements of a data migration plan. Although data migration may vary in complexity, the objective is that the integrity of the data is not compromised and that its context value remains.

For a successful migration, it is important that there is a good understanding of the data that exists in the current system. All possible data sources for the migration should be identified, and extractions and queries should be used to assess the 'cleanliness' of the data. The rationale for cleansing the data should be documented.

User requirements are formulated for the desired functionality of the data on the target system. If the target system is already in use in the production environment, care should be taken to ensure that there is no discrepancy between the user requirements and the existing functionality. A plan to deal with discrepant data (e.g., different blood groups on a given patient) should be documented and followed.

A migration specification document must be created describing the mapping of the fields from the old system to the new system. The document should also contain all necessary translations and/or modifications of database fields during the migration process.

All migration steps, as well as actions between the extraction and the import, must be documented in the data migration plan. If it is necessary to perform additional actions on the target system (i.e., on the imported data or the system as such), these actions should also be included in the document. Data migration requires several steps and should include verification of the data to ensure that the data being migrated is correct and in the proper format for use in the target system. There may be considerable differences between the database structure of the source system and the target system. The format and the functional usage of data in the receiving system can be significantly different; for example, limitations in the field length can create severe data integrity errors.

Execute and report

Once the data migration plan is written and approved, migration test runs should be performed in a test environment. For achieving an effective data migration procedure, data on the old system is mapped to the new system providing a design for data extraction and data loading. The design relates old data formats to the new system formats and requirements. The migration may involve many phases, but it minimally includes data extraction, where data is read from the old system and data loading, where data is written to the new system.

Iterations are part of the execution of the migration process. Prior to any iteration, parameters, translation tables, and code should be frozen to provide a stable platform for the iteration. Once the data is transferred, it must be verified. If corrupted data is identified, scripts must be corrected and data migration testing repeated.

Each iteration of the process should at least include these control check points:

- collation of migration process timings (extraction, transmission, transformation and load);
- continual identification of data cleanse issues;
- confirmation of parameter settings and parameter translations;
- identification of any migration merge issues;
- reconciliation and
- deviations.

The execution of a data migration process should be consistently repeatable and accurate. The data migration process should be repeated until it reaches consistent results and meets the requirements set in the data migration plan. Once the migration test runs are completed and the data accurately and completely translated, the integral end-to-end data migration process, as described in the data migration plan, can be performed in the production environment.

Perform migration verification in the production system

After loading into the new system, results are subjected to data verification to determine whether data was accurately translated, is complete and supports processes in the new system. During verification, there may be a need to run both systems in parallel to identify areas of disparity and prevent erroneous or lost data.

Points for consideration are:

- Is all user data correctly converted to the new format?
- Are there any missing records or fields?
- Are new fields initialized to correct values?

One of the methods for testing and verifying results is sampling. In addition, there are manual inspections that examine the results of a migration and process checking, which, unlike sampling and inspections, focuses on verifying that the tool or script used to move the data works as intended.

The migration plan is executed, and the process and migrated data are validated. Ideally, validation should be performed on the production system. In some cases, this is not a possibility. This situation can arise when the production system is in use or because validation requires manipulation of the imported data that cannot be reversed. It may then be necessary to perform the validation on a copy of the production system. In this case, the validation report should contain a precise description of the differences between the validation and the production environments and the impact the differences may have on the validation result.

When validation has been performed on a copied system, the actual migration can subsequently be performed with minimal testing on the production system.

It is important after successful data migration that the access to data in the old system is locked. This does not prevent access to the data by authorized, knowledgeable staff; it prevents modification of the data.

Data integrity

Data Integrity is the accuracy and consistency of data stored in a database, data warehouse or other similar data storing constructs. Data Validation comprises the tests and evaluations used to determine the correctness and reasonableness of data. It is not feasible to check all data during a validation. A sampling of data, the size of which is determined by risk analysis, should be performed.

General expectations

Data types. In a computer application, the data types are classifications of data such as Character, Number (integer or real numbers), Boolean and Date (date or date and time). Validation test cases must ensure that data types stored will be data types retrieved.

Data elements. Data elements are basic units of information built from standard structures having a unique meaning and distinct units or values. Examples of data elements are customer name, address and date of birth. Validation test cases must ensure that data elements stored will be data elements retrieved.

A record. A record is data associated with a given item (e.g., product, donor, patient, instrument). It consists of a group of data elements assembled in a particular order and with the same data types. Validation test cases must ensure that records stored in their entirety will be retrieved without compromising data elements in the record and their associated data types.

Count. The number of records stored in the database. Validation test cases must ensure that the number of records stored equals the number of records retrieved.

Record updates. An update to a record is changing the record to reflect new information. Validation test cases must ensure that similar data types are updated with compatible data types and that the key data fields are not modified. For example, the date of birth cannot be updated by an integer or character; similarly, a number cannot be updated to a character data type.

Deletes. A deleted record is when information is removed from the record. When computer application requirements allow deletion, the validation test cases must prove that deleted records are not retrieved.

Related records. A primary record is a unique identifier. Information associated with a primary record is captured in the related record(s). For example, a donor or patient identifier is a primary record, but there may be multiple addresses (related records) associated with the identifier. The validation test cases must prove that primary records and related records are retrieved as expected.

Dangling records. A dangling record is a record that has become disassociated with the primary record. When a primary record is deleted or deactivated, the related records must be deleted or deactivated accordingly. If a related record is not deleted or deactivated, then a dangling record exists in the database. The validation test cases must prove that there are no dangling records in the database.

Truncation. Truncation is when a data element is abbreviated. When the stored data in a data element is larger than the field can hold, information may be lost. Validation test cases must prove that truncation is accepted or rejected depending on the requirements.

Calculations. Calculations are when an input to a data element is converted before storing it in the database. The validation test cases must ensure that the retrieved value is equivalent to the entered value. For example, an employee's weekly work hours may be stored as seconds in the database, but when retrieved from the database, the data element is accurately displayed as hours.

Algorithms. An algorithm is a sequence of instructions where the main goal is to solve a problem. For example, calculating donor eligibility based on the last donation date or deferral information. The validation must ensure that the algorithm works as expected.

Encryption and decryption. These terms express the process of converting data to prevent unauthorized access to digital information. When the input to a data element or the entire record is encrypted before storing in the database, it must be accurately decrypted back to its original value.

Zero-size database

When a computer application is launched with a zero-size database—meaning there is no history or any existing data in the database—validation test cases must prove that:

- new data captured in the database is mapped properly to data types; for example, characters to character, date to date, number to number, etc.;
- the number of records entered is equal to the number of records stored;
- the number of records stored is equal to the number of records retrieved;
- updates applied to data elements are reflected when the record is retrieved and
- retrieved records exactly match the stored data elements in each record.

Converting the existing database to the new database

It is common practice to convert an existing database to a new database when:

- a new computer application is launched;
- the existing computer system is modified;
- the database provider has a major upgrade;
- there is an upgrade of the hardware and

- there is an upgrade of the operating system.

When converting (or migrating) to a new database, the validation test cases must prove data integrity by verifying the following:

- the number of records for each component (often known as tables) in the old database is equal to that in the converted (new) database;
- the required data elements have been migrated properly to the new database;
- data types are mapped properly in the new database;
- no truncation or loss of data has occurred in the new database;
- no loss of precision has occurred in the new database (e.g., 3.44445 is converted as 3.44445) and
- no loss of referential integrity such that there are no dangling records (for example, all donated units must be associated with a donor).

Additional data integrity checks may include the following match between the old and new databases:

- Number of donors;
- Number of blood donations for each donor;
- Number of donors by gender;
- Number of donors by postal code, city and state;
- Number of donors by each blood group and Rh type and
- Number of donors in each age group (e.g., 18–25, 26–30, 31–40, 41–50, etc.).

Additional record sampling validation

Automated reports. Test cases must include automated reports that ensure data integrity.

Reports and queries: when reports and/or queries are available in the computer application that is designed to extract data from the database, these reports or queries must be tested to verify each data element.

Manual verification. Test cases must include manual verification when automated reports are not possible (e.g., counting the number of Group O units in inventory manually to verify the number of Group O units in the electronic inventory is correct).

Manual spot checks of data elements. It is important to consider including validation test cases for manually spot-checking data elements. For example, it is reasonable to use the following guidelines for sample size as appropriate based on risk analysis.

- If the database size is in thousands, consider 1% to 2% of records for spot checks.
- If the database size is in millions, consider numbers like 500–1000 records selected randomly or by an algorithm (e.g., one out of every 100 donors in an alphabetical list) to perform spot checks.
- Special cases: If there are known special cases, run reports or queries against select special cases and perform spot checks.

Infrastructure qualification

IT infrastructure refers to the composite hardware, software, network resources and services required for the existence, operation and management of an enterprise IT environment.

A separate Performance Qualification is not expected for infrastructure as the PQ of the infrastructure is included in the OQ and PQ of the application(s) using the infrastructure.

The following hardware components (physical or virtual) are part of the IT infrastructure:

- connectivity elements [Local Area Network (LAN), Wireless Fidelity Network (WIFI) and Wide Area Network (WAN)];
- connectivity infrastructure that includes active and passive components. (Examples of active components are repeaters, switches and routers. Passive components include cables, connections and outlets.);
- servers enabling office automation that manages business applications, databases and data storage;
- workspace clients, such as thin or fat clients, personal computers, handhelds and
- peripherals (for example, scanners, printers and label printers).

In addition to visible physical components, IT infrastructure includes software. Software may:

- be central office automated services, like mail, file and web services. These services are not directly related to business applications;
- control the hardware (operating systems, firmware);
- be used for processing, storage and transport of data (databases, interfaces);
- manage the communication with the users (user interfaces, web servers);
- control the security of the system or
- manage virtual platforms.

When qualifying cloud services [particularly infrastructure as a service (IaaS) and platform as a service (PaaS)], the importance of qualifying the supplier becomes evident; in many situations, it is not possible for the organization to actually perform the qualification actions. Suppliers may not be keen on sharing their inside information (necessary for IQ/OQ activities) with customers for security reasons.

When qualifying the supplier, the emphasis is on reports from third parties regarding General IT controls (for instance, ISO 27001 certification and/or ISAE 3402 reports).

A prerequisite to ensuring a controlled and validated automated system is a qualified infrastructure including servers, networks and clients and other devices that are part of the network. This provides the foundation upon which the automated system, that is, the GxP application runs in an environment that is continuously maintained and in control.

Normally the infrastructure is qualified with an IQ and sometimes OQ. The PQ of the infrastructure is performed during the validation of the application(s).

According to GAMP®, recording version numbers and verification of correct installations are sufficient for qualifying infrastructure software, which is composed of established and commercially available layered infrastructure software (upon which the automated system application is built). The documentation and tests described below can be included in the validation of the application. At least minimal testing is needed for infrastructure qualification since proving the application runs correctly using the established infrastructure is what is important. A risk-based assessment approach should be used.

Servers

Qualification deliverables for servers should be limited to the equipment and its associated operating system and utilities. System upgrades require updated documentation and possible retesting.

- Requirements Specification should specify the functional requirements for servers and their operating systems and utilities.
- Design Specification should specify the actual configuration and setup of the equipment, operating system and utilities of the servers.
- Installation Qualification should:
  - capture the installation of the server. Serial numbers and models should be included. Any additional components not installed by the manufacturer should be documented
  - include the operating system, patches and upgrades, additional utilities and toolkits
  - Include start-up and shutdown procedures.
- Operational Qualification should include, at a minimum: the process of backup and recovery, data archival and retrieval (if applicable), critical aspects of security, functionality of the uninterruptible power supply, communications between servers and interfaced equipment, existence according to design of any system redundancy (such as mirrored drives) and secondary/failover systems.

Network infrastructure

- The network infrastructure can be defined as transportation and communication systems. Testing of the Wide Area Network (WAN) and Local Area Network (LAN) should be limited to the major components of the WAN/LAN. The network infrastructure is a dynamic environment; therefore, it is necessary to establish and follow good engineering, documentation and quality assurance practices. Network upgrades require updated documentation and possible retesting.
- Requirements Specification should (1) specify the functional requirements for the major components of the WAN/LAN infrastructure and (2) specify the required redundancy of the infrastructure.
- Design Specification should specify the actual equipment for the major parts of the WAN/LAN infrastructure. It is a description of the physical hardware components, such as hubs, switches, routers, patch panels and of the software components, such as transport protocols and network operating systems. WAN/LAN interfaces are included; other components, such as cabling, power supplies and interface cards, should also be captured.
- Installation Qualification should (1) capture the physical installation of the major components. Serial number and model should be included. (2) include the documentation of software on standalone switches and routers.
- Operational Qualification should use automated test equipment to verify that the appropriate security levels and filters are operating correctly and that the cabling works according to the requirements.

Clients

Where possible, organizations should be in control of the clients by disabling administrator rights for non-IT department users. The clients should be controlled via policies, procedures, CD images and audits. System upgrades require updated documentation and possible retesting.

- User Requirements Specification should (1) specify the functional requirements for the type of client workstations and laptops and (2) document the organization's standard type of clients and the minimum hardware requirements, as well as the current operating system including its patches, upgrades and software to be used.
- Installation Qualification should record system information (type of hardware, serial number of image/build in accordance with the established procedure).
- Operational Qualification should be performed by testing the applications running on the client in order to ensure that the applications operate according to their intended use in the client/server environment.

Qualification of virtual computerized systems

A virtual machine (VM) is an image file that exhibits the behaviour of a separate computer, capable of performing tasks such as running applications and programmes like a separate computer.

Qualification of virtual machines can be conducted as for non-virtualized systems while effectively mitigating the specific risks.

While considering risks associated with a virtualized environment, some of these risks are the same as for all other items of infrastructure; however, the complexity of the virtualized environment means that additional failure modes must be considered and that risk likelihood and detectability must be reconsidered.

Specific risks:

- Because of complicated data backup/restore procedures, there is a risk of corrupt, incorrect or lost data in certain parts of the virtual environment (e.g., wrong Storage Area Network, restoration to a wrong storage location, misconfigured failover resources);

- Suppliers may not support applications which are not designed for a virtual environment;
- There may be a dependency on a supplier to manage access to the platform and servers and
- Since physical network connections are replaced by virtual networks (VLAN), security risks to consider are (1) incorrect configuration of VLANs and (2) faulty interconnections between virtualized systems.

Complete virtual machines (including virtual hardware, operating systems, prerequisite software and configuration) can be qualified once and deployed many times in a consistent and repeatable manner.

Training

All personnel developing, maintaining or participating in the qualification process must be trained before beginning any validation activity in accordance with the facility training policies.

A plan must be developed to ensure staff are trained on the various functions they will be performing and that they are declared to be competent. It should be specified who requires training, at which level they have to be trained, and the documents on which the training is based. The choice of the appropriate training methods will be determined based on system complexity, the tasks to be performed and the background of the trainees. Suppliers may provide training support.

Once training documentation and SOPs are written and the automated system installed, training can be performed with or without instructors. It must be supported with clear training instructions and concurrent documentation of the training. The competency of the trained staff should be evaluated and documented. By the completion of training, operators should be able to perform the intended functions and respond in an appropriate and timely manner to all alarms, warnings and error messages.

Testing

Prior to testing, the system must be configured and frozen, and a change control mechanism must be established. All documents required for the qualification phase as defined in the validation plan must be available.

The results from testing should be documented on the validation protocol or an annex document against predefined acceptance criteria stated in the test instructions. Test anomalies should be captured and reviewed with the outcome documented (see Problem resolution).

The following rules for testing must be applied:

- All test results should be recorded indelibly.
- Any corrections should be performed according to the rules specified in the QMS of the institution, and a reason for the change should be specified if not obvious to an auditor of the information.
- Shorthand notations such as ticks should be avoided.
- Test results should be directly documented as testing occurs and should be retained (e.g., screen prints, reports, queries). Suppliers may provide documentation of validation testing electronically by means of grids with each step, acceptance criteria, interpretation and documentation of results using a screen print.
- Problem logs and resolution should be maintained.
- Testing summaries should be established.
- Test results should be reviewed and approved by a competent, independent person(s).

Problem resolution

All problems encountered during testing should be documented. Problems will fall into two categories: validation test case failures (for example, the system does not perform as expected, operator input errors that cause a test failure, errors due to configuration settings, outcomes that are not as expected but are acceptable) and test cases are inappropriately written.

Validation test case failures. The following tasks must be performed:

- documentation of all incidences of test case failure;
- investigation of all incidents to determine if:
  - the test case was properly written;
  - there was user error in executing the test case;
  - there was a specification error or
  - there was a system limitation.
- reporting of software programming problems to the vendor;
- identification of a solution (e.g., workaround, reconfiguration);
- documentation of resolution and
- depending on the change required to fix the problem, determine if only the test case should be re-executed or if regression testing of several functions is required. A risk assessment-based approach should be used to determine the amount of additional testing to be performed.

Validation report and final review

The validation report presents the results of the validation activities, including data migration, interpretation of the validation outcome and the conclusions drawn. If unexpected outcomes are obtained, they should be summarized. The summary should define what changes and/or 'workarounds' will be needed to mitigate the risk.

The final review is performed by staff identified in the validation plan upon completion of the validation process and consists of reviewing documents as specified in the plan. The review should confirm that:

- the documentation is complete;
- the testing proves, with a high degree of assurance that the system will consistently meet its acceptance criteria;
- data migration is complete and accurate;

- any non-conformance was addressed through problem-solving;
- training requirements have been met and
- a disaster recovery plan is in place.

The possible outcomes from this review are:

- release (go-live),
- conditional release (go-live with issues that do not impact patient safety, product quality and data integrity) or
- do not release.

The system can only be released by qualified personnel. If the system cannot be released or can only be conditionally released, the reason for the decision must be documented. In all instances, the decisions made must focus upon the importance of patient and product safety and data integrity.

After release, the facility is responsible for maintaining the validated state of the automated system according to pre-established plans.

Go-live process

Go-live is the process of going from project to operational status. This involves a transfer of responsibility from the project team to operational staff. The transfer process scope, acceptance criteria and transfer checklist should be established beforehand. Transfer activities performed should be described and approved paying special attention to the communication of open issues and incomplete activities or documentation. A period of monitoring the system after go-live is needed, and a rollback strategy is defined for serious problems emerging. The formal acceptance of the automated system and controlled transfer into the live operational environment should be documented.

ON-GOING ACTIVITIES

Disaster recovery plan (DRP)

A Disaster Recovery Plan (DRP), part of a business continuity plan, is required and consists of a number of elements designed to minimize disruption to the business in case of system failure/unavailability. An approach based on risk assessment is recommended. The following is recommended:

- Prepare a countermeasure plan to first identify risks and then mitigate those risks. This can include hardware redundancy, maintenance, system monitoring and data backup procedures, training and security arrangements.
- Prepare a DRP detailing how the system will be recovered and brought back into operation.
- Define the responsibilities of business, IT and IT suppliers.
- Periodically test the DRP.
- Identify individuals within a command centre for managing the disaster process. There must always be a team of experts (DR Team) in control of the DRP. The leader of this team must have enough authority for decision-making.

A **DRP** should consist of the following phases:

1. *Activation and notification phase*: Activation of the DRP may occur during planned events or after a disruption or outage that may extend beyond the Recovery Time Objective (RTO). The RTO is defined by a Service Level Agreement (SLA) for a system.
   The DRP team will notify application owners and process owners of the situation and (if applicable) about a possible long-term outage.
2. *Assessment phase*: Once the DRP is activated, perform an outage assessment and impact analysis for the system. Present findings from the outage assessment to a central disaster management team.
3. *Determining appropriate steps*: Based on the impact analysis, determine which disaster recovery steps will be invoked. Where the plan does not cover the situation, define appropriate measures.
4. *Recovery phase*: Implement the activities and procedures for recovery of the affected environment. Notify and escalate procedures for communication of recovery status to application owners and process owners as needed. Verify that alternate computerized systems used during recovery are working as intended.
5. *Reconciliation phase*: Reconciliation begins when operations return to their normal status. Perform actions to verify system capability and functionality has been restored at the original or new permanent location. Verification procedures may include functionality or regression testing, operational testing and/or data verification. At a minimum, the primary system's capability and functionality are verified. The system is declared recovered and operational upon successful completion of verification testing.
6. *Deactivation phase*: The deactivation phase includes activities to notify application owners and process owners. This phase also addresses recovery effort documentation, activity log finalization, incorporation of lessons learned into plan updates, readying resources for any future events and discharging the Disaster Management Team.

Validation state maintenance

Maintaining the validated state is one of the most difficult activities in guaranteeing the regulatory compliance and fitness of the use of an automated system. The maintenance phase spans the time between the automated system's start-up and the retirement of the system. The following items, which are essential to maintaining the validated state, may already be covered within the facility's quality system:

- preventive maintenance;
- incident management;
- software patches/service packs installation;
- training and competency;
- supplier requalification;

- periodic review;
- performance monitoring and
- system retirement.

Operational change control, document control and quality control procedures support the maintenance of the validated state.

IT equipment preventative maintenance

All critical equipment should have regular, planned maintenance to detect or prevent avoidable errors. This Planned Preventative Maintenance (PPM) should include routine day-to-day and periodic maintenance. PPM will ensure that the equipment required for any process remains in its optimum functional state.

- All equipment that requires PPM should be identified.
- Maintenance intervals should be determined for each item of equipment.
- The maintenance status of all equipment that requires PPM should be readily available.

Software patches/service packs installation

Transfusion services and donor centres work with software that may be regulated by the national competent authority, as well as software resources that are not regulated. The unregulated software and hardware provide the infrastructure for data transfer and connectivity between systems. Making changes to the software to update new functionality, installing security patches to minimize an identified vulnerability or adding new software to fix a software bug all require standardized processes and procedures. Facility change control policies and procedures apply to these changes. These requirements include the need to:

- assess the risks of making or not making the changes;
- document the decision-making and testing performed and
- monitor the system after the change is made.

This evaluation helps to determine the need for IQ, OQ and/or PQ. What differs between installing a new system and installing a patch to a system is the scope of the validation necessary to maintain a safe system. These requirements do not change regardless of the perceived urgency of implementing the update or software patch.

Timing of implementation. The urgency of implementing software is related to the level of need for the security of the system. Table 3 outlines urgency levels and appropriate actions.

Blood establishment software. It is unlikely that changes to the blood establishment software are critical for IT security. The standard process for making changes should be followed. There is time to assess the risks and perform testing before implementation in a process that meets all regulatory requirements for pre-implementation validation.

Security patches to the infrastructure. Security breaches are common, and software developers frequently issue updates and patches as frequently as weekly or when defects are found and a countermeasure created. Infrastructure changes can be planned or may come as an urgent patch to prevent a security breach. The institution should have a policy that outlines the risk assessment and approval processes for implementing a change at any level of risk or urgency. Regardless of the extent and urgency of the requested change, the risks need to be assessed and the decision documented.

TABLE 3 Actions indicated based on urgency levels for software implementation

Urgency level	Action
Patch or fix is optional	Assess the need for the fix and plan routine validation if required
Routine patch	Routinely scheduled, includes a review manufacturer's information, risk assessment and testing before implementation
Urgent security or operational fix to ensure data integrity	Review manufacturer's information, assess risk, notify users, implement, test critical functions
Mission critical security issue	Review manufacturer's information, implement, notify users, assess for negative impact, test critical functions

Blood establishment software is connected to other systems and is supported by the information technology infrastructure. This makes the system vulnerable to outside disruption and security breaches. The failure to handle the patch in a timely manner creates its own risks, and compliance with regulatory requirements is compromised.

The amount of validation testing performed is based on the risk of not making the change versus the risk of negative outcomes if the change is made. Routine and urgent implementation of patches and fixes should be:

1. scheduled;
2. placed into a test environment and
3. tested before implementation.

Only mission-critical software may be deployed without notification to the blood establishment. Any incident where software was deployed to end users without notification should be reviewed to ensure there was adequate documentation of the event and justification for implementation without notification and testing.

Review of manufacturer's release notes. The manufacturer's information about the changes provides details on how the changes affect the operation of the software and hardware. Some changes may provide the facility with a choice of options. The facility needs to determine if and how these changes impact their operating procedures and determine which, if any, option will be deployed. Based on this information, the risks of making the changes can be assessed, and a validation plan could be developed.

The goal of the patch may be to reduce a security risk or allow a mission critical task to continue. The risk analysis is still performed and documented as it is an important part of the decision-making process.

In some instances, the manufacturer may have limited information on the change or the downstream impact on the current system configuration. The extent of post-implementation testing and monitoring may increase when the deployment is done quickly and or with minimal or no information from the vendor.

Responsibilities. The facility's policies and procedures should define the groups or individuals responsible for the implementation. The facilities infrastructure team may be responsible for assessing the risks, documenting the decisions made and implementing the changes needed. Communication of the changes is a critical part of the process, even if making the changes is urgently required. The systems connected by the infrastructure may be adversely affected by the change. Communication is critically important when third parties have been contracted to manage the infrastructure or components of the system.

Versioning

In order to provide tracing and tracking computer applications it is necessary to uniquely identify the version of the application and module or programme units within the application. Methods of numbering versions may be found in Appendix C.

Training and competency

The ability of staff to use and support an automated system correctly should be maintained. The training programme should be reassessed for any critical change in environment, process or to the automated system.

The training programme should be adapted for each significant staff reassignment or newly assigned task related to the automated system.

Training records, including plans and protocols of the training status, ensure that training needs are properly identified, planned, delivered and documented for the entire validation process.

Suppliers of IT services may need to be trained in GMP requirements.

Supplier requalification

The frequency and the detail of the requalification process depends on the level of risk from using the automated system. Requalification should be planned for every supplier concerned.

This process can be performed through an audit similar to the one used for system selection. An internal procedure should be written to describe the level of auditing required for re-qualifying suppliers based on the purpose of the audit.

Supplier's requalification is not limited to the audit; it also concerns the follow-up of audit findings.

The decision to continue with a supplier will depend on the criteria established by the blood establishment and the level of compliance to the regulatory requirements applicable in the country concerned.

Periodic review

The aim of the periodic review of computerized systems is to establish that procedures continue to meet requirements and are approved. The review also confirms that qualification documents are complete, current and accurate.

Elements of the system should be verified before implementation and reverified at regular intervals as defined by the facility. The frequency of verification intervals for elements can be determined based on risk assessment.

A periodic review should be planned and scheduled to comply with the guidelines of the competent authority. The facility should define the scope, depth and frequency of the periodic review assessment.

It should consider:

- specification and design of components (Are specifications in place?);
- asset list (Is there a configuration item list, and are physical components in place and updated?);
- qualification documents (Was the OQ in accordance with qualification plans? Was the qualification testing based on risk assessments?);
- change management (Are procedures in place including consideration of the need for testing?);
- security management (Are virus protection and firewalls in place and maintained? Are there reports of security issues? Are physical and logical controls in place?);
- incident and problem management (Is there a process in place for reporting, assessing and documenting? Is there an overview of incidents and problems?);
- backup and recovery (Are procedures in place, tested and assessed against requirements?);
- disaster recovery (Is the process defined, tested and documented?);
- supplier qualification (Are suppliers assessed against quality requirements? Have there been any changes in procedures with suppliers?);
- changes in the environment, process, business requirement, legislation or accepted best practices;
- personnel qualification, training and competences;
- documentation for using and supporting the system (Are there policies, processes, procedures, operational plans and related records) and
- audit reports.

A report of the review process should be prepared and should include:

- relevant results obtained;
- deviations or problems found;
- required corrective actions and
- the ratification of the continued acceptability for the system use.

Identified actions should be prioritized and planned. A risk assessment-based approach should be used.

A date when the computerized system is due for periodic review/re-validation should be established.

Performance monitoring

To ensure the proper operation of an automated system consisiting of computers, networks and applications, a monitoring plan should be developed and implemented to ensure the proper operation of an automated system consisting of computers, networks and applications. The plan should take into account the criticality of the system being monitored and outline monitoring, user notification and problem-solving mechanisms.

Critical system conditions should be monitored with suitable monitoring tools at appropriate time intervals. The monitoring plan should state acceptable and unacceptable system parameters, the monitoring tool to be used and the frequency of observation.

If an unusual event is observed, personnel should follow the standard response outlined in the monitoring plan. The standard response will likely involve notifying affected personnel and initiating a resolution to the problem. Depending on the severity of the problem and the criticality of the system, backup and restoration plans may need to be implemented. See Disaster Recovery Plan (DRP).

System retirement

At the end of the operation, the automated system should be decommissioned. The following rules should be applied:

- If the retirement of the automated system involves a replacement, it should be planned.
- Consideration should be given to archiving system software.
- If the data is archived, it should be done in such a way that it can be retrieved and read during the required time frame unless the data is migrated to a validated replacement system.
- An archive report should be generated describing the archive approach and listing the documents, raw data and electronic records archived.
- It may be necessary to retrieve the data independently of the original system.
- The data should be retained as required by the regulations and company policy.

SECURITY

Security policies should be developed for defining the rules and guidance regarding the use and access to critical information. It could be performed through the Guidelines on Information Security from ISBT.

User access policies

User access policies should be developed requiring unique identification codes for each user, periodic password changes, prohibition of sharing passwords and mechanisms to ensure users are added to and deleted from the system as appropriate and when authorized. Users should have access only to the information they need to perform their job duties. Appropriate measures should be taken against unauthorized input, deletion or modification of critical data. Any deviations and/or modifications to these access policies will be documented and approved.

System access policies

System access policies should be developed in order to protect the system from unauthorized access. They should include:

- physical security;
- system access security, including user access;
- e-mail systems;
- shared network resources;
- internet access and use;
- system network connection security;
- software licenses and
- external automated systems.

Procedures should describe how the policies are implemented.

BACKUP AND RECOVERY

To ensure the availability and reliability of stored electronic data, backups should be

- made to reconstruct GxP relevant records;
- routinely performed as defined by the Quality Management System and any existing Service Agreements (e.g., the backup process, the number of backup copies, the frequency of backup, the backup verification process and the restore process) and
- performed before any significant software changes.

This applies to any system, including software, environment configuration and operating system.

- The backup process should ensure data integrity; each backup should be verified that it is complete and error-free.
- Physical backup copies should be stored in a secure place and in an appropriate environment (protected from fire, water and other hazards) that guarantees the quality of the storage medium and complies with confidentiality and privacy regulations and should be stored in an offsite location.
- Each backup medium should be clearly identified, for example, CD, tape, cloud.
- A log of backups should be maintained.
- The method of restoring and establishing control should be specified in the event recovery is required.
- The recovery process should be validated and routinely tested.

ARCHIVE AND RECORD RETENTION

All information produced within a critical automated system should be managed according to defined processes and with appropriate support.

A records retention policy and its use should be established. The type of records should be documented as well as the defined period of retention for each.

Archiving of electronic records involves the use of offline electronic storage. The archive process to follow should be documented, and consideration should be given to the following:

- documentary evidence to be taken when records are archived;
- indexing facilities;
- data should be secured by physical and electronic means against willful or accidental damage;
- storage facilities and environmental conditions should minimize the degradation of record storage media that could result in the loss of data;
- archived data should be secured in a manner that satisfies confidentiality and privacy regulations;
- electronically stored records should be periodically regenerated, based on the specification of the technology used;
- retained or archived records should be readily retrievable for business or regulatory purposes and
- access to the hardware needed to read these media needs to be maintained.

ACKNOWLEDGEMENTS

This is the third version of validation guidelines written by the ISBT Working Party on Information Technology. The previous two versions were entitled: ISBT Guidelines for Validation and Maintaining the Validation State of Automated Systems in Blood Banking (Vox Sang 2003; Suppl 1:S1–14) and ISBT Guidelines for Validation of Automated Systems in Blood Establishments (Vox Sang 2010;Suppl 1:S1–19). The authors of this third version would like to thank the writers of the earlier versions for their contributions, many of which are continued in this version.

All authors contributed to the literature research, writing and editing of the document. JWA was the chair of the Validation Task Force of the WPIT. SB was the Chairperson of the WPIT.

The Validation Task Force thanks the ISBT for the opportunity to work on these guidelines.

FUNDING INFORMATION

Funding for face-to-face meetings was provided by ISBT.

CONFLICT OF INTEREST

The authors declare that there is no conflict of interest.

ORCID

Jan-Willem Andriessen https://orcid.org/0000-0001-5195-8583
Patricia Distler https://orcid.org/0000-0002-7848-3554

REFERENCES

1. GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems. ISPE. 2010.
2. GAMP Good Practice Guide: IT Infrastructure Control and Compliance. ISPE. 2017.
3. GAMP® 5 Guide: A Risk-based Approach to Compliant GxP Computerised Systems. ISPE. February 2008.
4. ICH guideline Q9 on quality risk management. 2022. Available from https://www.ema.europa.eu/en/documents/scientific-guideline/international-conference-harmonisation-technical-requirements-registration-pharmaceuticals-human-use_en-3.pdf
5. Good Practices for Computerised Systems in Regulated 'GxP' Environments. PIC/S - Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme. PI 011–3. 2022. Available from https://picscheme.org/docview/3444

How to cite this article: Andriessen J-W, Breard M, Briggs L, Butch S, Distler P, Georgsen J, et al. International Society for Blood Transfusion Guidelines for Validation of Automated Systems in Blood Establishments. Vox Sang. 2022;117:1420–45.

READING LIST

- 21 CFR Part 11 Electronic Records; Electronic Signature, Final Rule. Department of Health and Human Services - Food and Drug Administration. Part 11, Electronic Records; Electronic Signatures - Scope and Application | FDA (9 November 2021).
- GAMP® Good Practice Guide: A Risk-Based Approach to Operation of GxP Computerized Systems. ISPE. January 2010 GAMP Good Practice Guide: IT Infrastructure Control and Compliance. ISPE. August 2017.
- ISPE GAMP® Guide: Records and Data Integrity. ISPE. August 2017.
- GAMP Good Practice Guide: Testing GxP Systems. ISPE. February 2012 GAMP® Good Practice Guide: A Risk-Based Approach to GxP Compliant Laboratory Computerized Systems. ISPE. October 2012.
- GAMP® 5 Guide: A Risk-based Approach to Compliant GxP Computerised Systems. ISPE. 2008.
- General Principles of Software Validation; Final Guidance for Industry and FDA Staff. U.S. Department of Health and Human Services - Food and Drug Administration, Center for Devices and Radiological Health, Center for Biologics Evaluation and Research. http://www.fda.gov/cdrh/comp/guidance/938.pdf. January 2002.
- Glossary of Computerised System and Software Development Terminology. Inspection references: Inspection Guides. U.S. Food and Drug Administration Office of Regulatory Affairs. Glossary of Computer System Software Development Terminology (8/95) | FDA (9 November 2021).
- GLP Consensus Document the Application of the Principles of GLP to Computerised Systems, Environment Monograph N°116. OECD. 1995.
- GLP – Guidelines for the Validation of Computerised Systems. Working group Information Technology (AGIT). Version 2. http://www.bag.admin.ch/themen/chemikalien/00253/00539/03300/index.html?lang=en. December 2007.

- Guidance for Industry Cybersecurity for Networked Medical Devices Containing Off-the-Shelf (OTS) Software. U.S. Department of Health and Human Services Food and Drug Administration - Center for Devices and Radiological Health. January 2005. https://www.fda.gov/regulatory-information/search-fda-guidance-documents/cybersecurity-networked-medical-devices-containing-shelf-ots-software (accessed 1 December 2021).
- Guidance for FDA Reviewers and Industry – Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices. U.S. Department of Health and Human Services Food and Drug Administration - Center for Devices and Radiological Health. May 2005 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/guidance-content-premarket-submissions-software-contained-medical-devices (accessed 1 December 2021).
- Guidance for Industry Q10 Pharmaceutical Quality System U.S. Department of Health and Human Services Food and Drug Administration Center for Drug Evaluation and Research (CDER) Center for Biologics Evaluation and Research (CBER) April 2009 ICH https://www.fda.gov/media/71553/download (Accessed 1 December 2021).
- Guide to the Preparation, Use and Quality Assurance of Blood Components 14th Edition. CoE. 200.
- ISBT Guidelines for Information Security in Transfusion Medicine, Volume 91 Supplement 1 Vox Sanguinis. July 2006.
- ISO 9001:2015Quality management systems. Requirements. International organisation for Standardization. September 2015.
- Medical Device Quality Systems Manual - 5. Personnel and Training. U.S. Food and Drug Administration - Center for Devices and Radiological Health. http://www.fda.gov/cdrh/qsr/05prsnl.html. January 1997.
- Medical Device Quality Systems Manual - 15. Complaints. U.S. Food and Drug Administration - Center for Devices and Radiological Health. http://www.fda.gov/cdrh/qsr/15compl.html. January 1997.
- OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring - N° 10. Organisation for Economic Co-Operation and Development. https://www.oecd.org/officialdocuments/publicdisplaydocumentpdf/?cote=ocde/gd(95)115&doclanguage=en. (9 Nov 2021).
- PIC/S Good Practices for Computerised Systems in Regulated ‘GxP’ Environments Guidelines 25 September 2007.
- PIC/S GMP Guide to Good Manufacturing Practice for Medicinal Products Part II. PIC/S - Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme.
- PIC/S Validation-Master Plan, IQ, OQ, non-sterile Process Validation, Cleaning Validation (PI 006-3) Sept 2007.
- Q8(R2) Pharmaceutical Development U.S. Department of Health and Human Services Food and Drug Administration Center for Drug Evaluation and Research (CDER) Center for Biologics Evaluation and Research (CBER) November 2009 ICH Revision 2.
- Risk Assessment Program Data Management Implementation Plan. Environmental Restoration Risk Assessment Program, Lockheed Martin Energy Systems, Inc. http://risk.lsd.ornl.gov/homepage/tm/tm232.pdf. November 1997.
- Validation in Blood Establishments and Transfusion Services. AABB Press. 1996.
- Validation Master Plan Installation and Operational Qualification Non-Sterile Process Validation Cleaning Validation. PIC/S Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme. PIC/S Validation-Master Plan, IQ, OQ, non-sterile Process Validation, Cleaning Validation (PI 006-3) Sept 2007 - ECA Academy (gmp-compliance.org) (9 November 2021).
- MHRA GXP Data Integrity Guidance and Definitions, 3/18. MHRA. March 2018.

ACRONYMS

BECS:	Blood Establishment Computer System
cGMP:	Current GMP
CMDB:	Configuration Management Database
DBMS:	Database Management System
DHF:	Design History File
DRP:	Disaster Recovery Plan
DR:	Disaster Recovery
DHR:	Device History Record
DMR:	Device Master Record
DS:	Design Specification
FDA:	Food and Drug Administration
FS:	Functional Specification
GAMP$^{®}$:	Good Automated Manufacturing Practice
GLP:	Good Laboratory Practice
GMP:	Good Manufacturing Practice
GxP:	Good ‘x’ Practice, where ‘x’ represents

- Clinical
- Quality
- Distribution
- Laboratory
- Manufacturing

IaaS:	Infrastructure as a Service
ICH:	International Council for Harmonisation of Technical Requirements for Pharmaceuticals for Human Use
ISO:	International Organisation for Standardization
IQ:	Installation Qualification
IT:	Information Technology
ISPE:	International Society for Pharmaceutical Engineering
LAN:	Local Area Network
OQ:	Operational Qualification
PaaS:	Platform as a Service
PPM:	Planned Preventive Maintenance
PQ:	Performance Qualification
QA:	Quality Assurance
QMS:	Quality Management System
RTO:	Recovery Time Objective

SLA:	Service Level Agreement
SOP:	Standard Operating Procedure
URS:	User Requirement Specification
UPS:	Uninterruptible Power Supply
VLAN:	Virtual Local Area Network
VM:	Virtual Machine
WAN:	Wide Area Network
WPIT:	Working Party on Information Technology

GLOSSARY

Automated system: Term used to cover a broad range of systems, including automated manufacturing equipment, control systems, automated laboratory systems, manufacturing execution systems and computers running on manufacturing database systems. The automated system consists of the hardware, software and network components, together with the controlled functions and associated documentation.

Client: An application or system that accesses a remote service on another computer system, known as a server, by way of a network. The term was first applied to devices that were not capable of running their own stand-alone programmes, but could interact with remote computers via a network. These dumb terminals were clients of the time-sharing mainframe computer. A fat client (also known as a thick client or rich client) is a client that performs the bulk of any data processing operations itself and does not necessarily rely on the server. A thin client is a minimal sort of client. Thin clients use the resources of the host computer. A thin client's job is generally just to graphically display pictures provided by an application server, which performs the bulk of any required data processing.

Computer system: A functional unit consisting of one or more computers, associated peripheral input and output devices and associated software that uses common storage for all or part of a programme and also for all or part of the data necessary for the execution of the programme; executes user-written or user-designated programmes; performs user-designated data manipulation, including arithmetic operations and logic operations and that can execute programmes that modify themselves during their execution. A computer system may be a stand-alone unit or may consist of several interconnected units.

Computerised system: Includes hardware, software, peripheral devices, personnel and documentation; for example, manuals and Standard Operating Procedures.

Critical safety patch: A software patch that is considered mandatory by the vendor. It typically improves security or mitigates a known threat.

Disaster recovery: A set of policies, tools and procedures to enable the recovery or continuation of vital technology infrastructure and systems following a natural or human-induced disaster. The disaster recovery plan includes policies and testing and may involve a separate physical site for restoring operations. This preparation needs to be taken very seriously and will involve a significant investment of time and money to ensure minimal losses in the event of a disaster.

Engineering diagrams: Description of the way a device is built. It could be electrical wiring schema, technical information, etc. Where information must be presented by means of a signal flow chart or circuit diagram, such visual aids shall be divided into discrete units, simplified and standardized.

Functional specification (FS): Description of the product to be supplied in terms of the functions it will perform and the facilities required to meet the user requirements. It covers mechanical, electrical layout, hardware and software elements. This kind of document is written in such a way that both supplier and user understand it.

Hardware design specifications: Description of the architecture and configuration of the hardware. It includes controllers, PCs, instrumentation and interfaces.

Installation requirements: Description of the environment into which the automated system should be installed.

Manuals/User guides: Documents describing the use of the system and the maintenance tasks that have to be performed by the user. It is a description of the product in terms of the functions it may perform and the facilities required to appropriately utilize the product.

Purchasing documentation: Document ordering any significant part of the automated system, including equipment, computer system or part of it and new development. It may be used for tracking the purchasing process.

Patches/Service packs: Code added to the software in order to fix a bug, especially as a temporary correction between two releases.

Process owner: The person ultimately responsible for the business process or processes being managed.

Qualification: The act of proving and documenting that equipment or ancillary systems are properly installed, work correctly and comply with specified requirements. Qualification is part of the validation, but the individual qualification steps alone do not constitute process validation (Qualification is an act or process to assure something complies with some condition, standard or specific requirements.)

Recovery time objective: The maximum tolerable time allowed for the recovery of a computer, system, network or application.

(IT) Services: The application of business and technical expertise to enable organizations in supporting their business processes

Software: Software is often divided into two categories: Systems software includes the operating system and all the utilities that enable the computer to function. Applications software includes programmes that do real work for users. For example, word processors, spreadsheets and database management systems fall under the category of applications software.

Software design specifications: Description of logical and physical structures of the programme, the standards to be used for file naming, label allocation and module naming. It defines how the software implements the requirements based on the functional specification.

Standard operating procedure (SOP): Written and approved description of essential steps, their sequence, responsibilities and precautionary measures necessary to assure that operations can be accomplished routinely and in a uniform manner.

Supplier audit report: Presentation of the results of the investigation of the adequacy of the supplier to assure the quality and the reliability of the supplied automated system.

User requirements specification (URS): Clear and precise definition of what the user wants the system to do. It defines the functions to be carried out, the data on which the system will operate and the operating environment. The URS also defines any non-functional requirements, constraints such as time and costs and what deliverables are to be supplied. The emphasis should be on the required functions and not the method of implementing those functions.

Verification: The process of checking that the software meets specifications.

Validation: The process of checking whether the specification captures the customer's requirements.

Validation master plan: Describes the areas of the company within which validation is to take place and provides an overview of the status of planning. It lists the areas, systems and projects being managed, defines the status of validation for each and gives a broad indication of when validation is to be completed. It is a general plan and would normally cover all production areas and/or processes. It should include all systems for which validation is planned.

Validation plan: Description of the validation activities, responsibilities and procedures. It describes specifically how the validation is to be done.

Validation protocol: Prospective experimental (testing) plan that, when executed, is intended to produce documented evidence that the system performs as intended.

Validation report: Presentation of the results of validation activities, interpretation of the results and the conclusions drawn. If unexpected results are obtained during validation testing, it defines what changes will need to be made or what workarounds will be implemented to mitigate risk.

Validation, concurrent: Validation is conducted when there is no possibility of completing a validation programme before releasing a product or part of it. In this case, all validation concerns should be documented prior to the release of the product.

Validation, prospective: Validation is conducted prior to the distribution of either a new product or product made under a revised manufacturing process, where the revisions may affect the product's characteristics.

Validation, retrospective: Validation of a process for a product already in distribution based upon accumulated production, testing and control data. Test data is useful only if methods and results are adequately specific.

APPENDIX A: SAMPLE QUESTIONS FOR SUPPLIER QUALIFICATION

1. Are you a supplier of Infrastructure or a Service organization monitoring Infrastructure? If "yes", please describe the type of infrastructure you supply and the certification process you have been qualified by. If "no", please complete the following questions.
2. Do you have a Quality Policy? Do you have a Quality Manual?
3. Is there a Quality Management System in place? What is your familiarity with ICH Q10 Pharmaceutical Quality System?
4. Is there a security policy in place for the system?
5. Has there been a previous Quality Audit which is a systematic, independent examination of your adherence to the Quality System? What were the findings?
6. Is there an effective communication and escalation process in place in order to raise Quality issues to the appropriate levels of management?
7. What part does the Management Team play in the intentions and direction and application of the Quality System to your product or service?
8. Are there SOPs for all of the Development, Implementation and Maintenance phases?
9. What is the Change Control Process employed? Has it been documented? Do you use a Version Control system that allows the users to use, test and validate the system without interfering with LIVE use? Is Design Control part of the process?
10. How do you use a product and process understanding to enhance understanding throughout the lifecycle of your product or service?
11. Is the system configurable and if so, how is configuration management controlled?
12. Do you have a DHF (Design History File) for the current finished device as it is today? DHR (Device History Record)? DMR (Device Master Record)?
13. Are there Functional Requirements that have been developed for the System?
14. Do you have adequate resources for design issues such as: assessing new products; training and retraining of design managers and design staff; use of consultants, evaluation of the design process; product evaluation, including third-party product certification and approvals; patenting or other means of design protection?
15. How do you ensure that your Design Specifications have been implemented in the System? Is there a final validation before release of the system? Enhancements tested as part of a new/upgrade Version? What documentation do you have that describes your design and development planning?
16. Has there been validation of the system with respect to the Functional Requirements of the finished product? What kinds of documentation has been developed for the Testing and Validation of the system? Validation Master Plan? Test Plans? Matrix Document: Requirements versus Test Scripts; Test Scripts
17. Is there a document control system in place?
18. Are there any other activities that you feel help to improve the Quality Assurance activities that prove the development and implementation of the system are under control?
19. Is the customer informed of planned changes, and is there an opportunity for the customer to validate the changes?

APPENDIX B: CLASSIFICATION OF AUTOMATED SYSTEMS

GAMP® 5 A Risk-based Approach to Compliant GxP Computerised systems [3] and the PIC/S Good Practices for Computerised Systems in Regulated 'GxP' Environments [5] categorize automated systems and the applied tasks as follows.

Category 1: Infrastructure software

Established operating systems are not subject to specific validation. However, functions used by a critical software application should be validated. The name and version of the operating system should be documented and verified during Installation Qualification (IQ).

TABLE B1 Classification of automated systems used in blood banking

Automated system	Automated system categories
Air handling systems	4
Alarm system	4
Apheresis machines	4
Automated component processing system	4
Autonomous computer system with critical information (e.g., laptop)	5, 4, 3
Balance/mixer	4
Barcode reader	1
Blood product storage devices	4
Blood pressure automated system	1
Centrifuge	4
Computer system (including emulator)	5, 4, 3
DBMS (Database Management System)	1
ECG machine	1
Electronic archive system	5, 4, 3
Electricity backup system, UPS	4
Electronic balance	1
Electronic thermometer	4
Fast freezer	4
Hb meter	1
Heat sealer	1
Incubator	1
Irradiator	4, 3
Analytic automated system	4
LIMS (Laboratory Information Management System)	5, 4
Network	1
Network device	4
Printer	1
Operating system	1
Software application	5, 4, 3
Tube docking system	1

Note: Some automated systems are classified under more than one category since they may have different configurations.

Category 2: No longer used

Category 3: Non-configured software

These are commercially available standard software packages where configuration is limited to establishing its runtime environment (e.g., network and printer connections). The name, version and any configuration should be documented and verified during Installation Qualification (IQ). Functionality and user requirements (e.g., security, alarm and event handling, calculations and algorithms) should be tested within Operational Qualification (OQ).

Category 4: Configured products

Configured products provide standard interfaces and functions that enable the configuration of user-specific business or manufacturing processes. The development process should be assessed through a supplier audit. The audit should focus on the quality system and that application and support organizations are robust and competent.

The name, version and any configuration should be documented and verified during Installation Qualification (IQ). Functionality and user requirements (e.g., security, alarm and event handling, calculations and algorithms) should be tested within Operational Qualification (OQ) and the Performance Qualification (PQ).

Category 5: Custom applications

Custom applications are developed to meet the specific needs of the user company. It may be a complete system or extension to an existing system. The development process should be assessed through a supplier audit. The audit should focus on the quality system and that the application and support organizations are robust and competent.

The name, version and any configuration should be documented and verified during Installation Qualification (IQ). Functionality and user requirements (e.g., security, alarm and event handling, calculations and algorithms) should be tested within Operational Qualification (OQ) and Performance Qualification (PQ).

Table B1 lists classifications of automated systems used in blood banking based on the system described above.

APPENDIX C: VERSIONING METHOD

The versioning may use a simple numbering sequencing scheme. In general, for the software application versioning will be applied for two entities (i) at the application level and (ii) at the programme-unit level (or module, package, script, etc.). The following will describe the convention.

At the application level, the following may be applied:

v[major release].[minor release].[identity]

Where: v – indicates version (always lowercase)

[major release] – a major release relates to when significant changes are made to more than one of the following: the application including drastic changes to look and feel, extensive new features, major technology upgrade such as database and/or operating system impacting full re-compile and other high-impact events as determined by the product development and support team.

[minor release] – a minor release related to one of the above conditions as stated in the major release. Typically, it would be a new feature added to the application having significant impact to the process and users.

[identity] – an identity refers to application status whether it is in alpha, beta, limited release or final release.

0 is for alpha status
1 is for beta status
2 is for limited release
3 is for production status

Examples:

1. v3.0.0 – at the application level means the software application is running at major version 3, minor version 0 and is at the alpha testing
2. v3.1.1 – means the software application is running at major version 3, minor version 1 and is at the beta testing
3. v3.2.3 – means the software application is running at major version 3, minor version 2 and is at its final release

At each program (or the Form, Module, Package, Script) level following will be applied:

FFFFFFFF rel: nnn ("rel" always in lower case)

Where:

FFFFFFFF – is the upper-case Program-Unit Name (the first 8 significant characters)
rel – represent production release of the Form
nnn – indicates release number of the Form

Example:

MODPROG rel: 004

Means MODPROG is the program-unit name
rel: 004 is the release number of the form MODPROG

Both Application and Program Unit put together.

The following string will describe the combined Application and Program Unit together.

MYAPP v3.1.3MODPROG rel: 004

meaning – MYAPP is at major version 3, minor version 1, in production mode 3 and currently running the form MODPROG with release level 004.

Internal Mechanics:

a. Application version may be stored in a controlled text file
b. fter connecting to the application, the initiating program may read the text file for App version
c. The version for program unit may be hard-coded in each program or stored in controlled text-file
d. When the program unit is launched within the App, it can read the text-file, match the program unit name to display the program version
e. When Application is launched through Windows, the title MDI will be formatted as below:

MYAPP v3.1.3MODPROG rel: 004 Login User: UUUUUU on MM-DD-YYYY HH:24MI.SS

Where:

MYAPP	is the application name
V3.1.3	is the application version
MODPROG	is name of the program Unit
rel: 004	is modification level for the program MODPROG
UUUUUU	is the user currently logged-in

MM-DD-YYYY HH24:MI.SS is the user login date and time with seconds

The program unit release history:

The program unit release history will display last 5 changes made to the program unit:

For example for the Form MODPROG, it will be: (CR may represent Change Request)

rel 001 CR17000021
rel 002 CR18000010
rel 003 CR18000012
rel 004 CR18000111