

Vox Sanguinis

The International Journal of Transfusion Medicine

Volume 85 Supplement 1 August 2003

ISBT – Guidelines for
Validation and Maintaining the
Validation State of Automated Systems in Blood Banking

Version 1.1
July 2003

This document has been written by the International Society of Blood Transfusion Validation task force

Wolfgang Böcker, Germany
Mike Clark, UK
Christian Desaint, France
Rodeina Davis, USA
Pat Distler, USA
Carlos Izaguirre, Canada
Angelika Kawaters, Germany
Bonnie Lupo, USA
Sue McDonnell, Ireland
Charles Munk, Switzerland (chairman)
Robin Nozick, USA

Table of contents

Foreword	S1
Acknowledgements	S1
1. Overview	S1
2. Purpose	S2
3. Scope	S2
4. Responsibility	S2
5. Change control	S2
5.1 Project change control	S2
5.2 Operational change control	S3
6. Validation process throughout automated system lifecycle	S3
6.1 Start up	S3
6.2 User Requirements Specification (URS)	S3
6.3 System selection	S3
6.3.1 URS review	S3
6.3.2 Supplier qualification	S3
6.3.3 System evaluation	S3
6.3.4 Financial Considerations	S4
6.4 Risk assessment	S5
6.5 Validation plan	S5
6.5.1 Validation approach	S5
6.5.2 Validation protocols	S6
6.6 Training	S7
6.7 Testing	S7
6.8 Business continuity plan	S7
6.9 Problem resolution	S7
6.10 Validation report and final review	S7
6.11 Validation state maintenance	S8
6.11.1 Calibration and monitoring	S8
6.11.2 Preventative maintenance	S8
6.11.3 Training and competency	S8
6.11.4 Suppliers re-qualification	S9
6.11.5 Periodic review	S9
6.11.6 Performance monitoring	S9
6.11.7 System retirement	S9
7. Security	S9
7.1 User access policies	S9
7.2 System access policies	S10
8. Back-up and recovery	S10
9. Archive and record retention	S10
10. References and reading list	S10
11. Acronyms	S11
12. Glossary	S11
Appendix 1 Documentation	S13
Appendix 2 Classification of automated systems	S14

ISBT – Guidelines for validation and maintaining the validation state of automated systems in blood banking

Foreword

For the last 20 years, the evolution and the use of technology have grown exponentially. In the 1980s, there was a gap between the need and what the industry could supply. In the 1990s this gap narrowed and the use of technology followed the development evolution. Now we are in a period where suppliers anticipate the needs of users.

The following questions now arise:

- what is the relationship between users and suppliers?
- does the supplied technology fit with user expectations?
- what is the guarantee that purchased technology will work as expected and that it can be used without risk?
- who is responsible for what?
- how can we optimize the cost of maintaining quality technology?

Validation is one answer to these questions and these guidelines intend to provide guidance for the application of the validation process for automated systems in blood banking i.e. those systems that have some degree of computer control.

The benefits of validation are to:

- improve the use of technology;
- improve the business benefits;
- improve the relationship between stakeholders (users, suppliers, authorities, etc.);
- improve operational efficiency;
- reduce the risk of failure;
- improve compliance with regulations.

These guidelines are not intended to present a new concept of validation. They are built upon other field validation experiences and adapted to blood banking needs considering:

- the size of the organization;
- the impact of risk in blood banking;
- the need to have reliable automation systems;
- the diversity of activities taking place in blood banking;
- the evolution and consequently, the constraint of regulations;
- the resources needed to implement a validation process.

The following were chosen as the main references for these guidelines:

- GAMP Guide for Validation of Automated Systems [1];
- FDA Guidance for Industry General Principles of Software Validation [2];
- PIC/S Validation Master Plan Installation and Operational Qualification Non-Sterile Process Validation Cleaning Validation [3];
- PIC/S Good Practices for computerized systems in regulated 'GxP' environments guidelines [4].

Acknowledgements

The Validation Task Force would like to thank the following organizations for their support.

America's Blood Centers, USA

Blood Bank of San Bernardino and Riverside Counties, USA

Blood Center of Southeastern Wisconsin Inc., USA

Canadian Blood Service, Canada

German Red Cross Blood Transfusion Service West, Germany

French National Blood Service, France

Irish Blood Transfusion Service, Ireland

International Council for Commonality in Blood Banking Automation, Inc, USA

International Society of Blood Transfusion

National Blood Service, United Kingdom

R. F. Nozick and Associates Inc., USA

Swiss Red Cross Blood Transfusion Service, Switzerland

Swiss Red Cross Regional Blood Transfusion Service, Vaud, Switzerland

The Validation Task Force is very grateful to Mr. Tom Conway for his comment and for reviewing the consistency of the guidelines.

Furthermore, we would like to thank especially the following organization for sponsoring the Guidelines publication:

Abbott Diagnostic

Baxter Switzerland

DiaMed Diagnostic

Haemonetics

Octapharma

F. Hoffmann-La Roche Diagnostics Division

Swiss Red Cross Blood Transfusion Service

1. Overview

Every blood banking organization should have a Quality Management System. This should include a section on

Correspondence: Charles Munk, Swiss Red Cross Regional Blood Transfusion Service, rue du Bugnon 27, CH-1005, Lausanne, Switzerland
E-mail: Charles.munk@hospvvd.ch

validation (e.g. Validation Master Plan) 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.

These guidelines address the validation needs for automated systems, i.e. those that have some degree of computer control. An organization's validation policy should comply with the regulatory requirements applicable in the country of use. 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' and should not be divorced 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, maintenance and calibration.

Validation requires a structured approach. The approach normally used for automated systems is based on the methodologies developed initially to manage software development; based on the concept of a computer system lifecycle.

A computer system lifecycle is defined as the period of time that begins when a system is conceived and ends when the system is no longer available for use.

Not all computerized systems consist solely of a computer and software. In many cases the computer system is embedded deep in a piece of process equipment such as an autoclave or analytical instrument.

2. Purpose

These guidelines have been developed by the Validation Task Force of the International Society of Blood Transfusion Working Party on Automation and Data Processing (ISBT WPADP).

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

This document does not intend to cover FDA regulations 21 CFR part 11 [5].

3. Scope

Validation must be performed on all automated systems that are considered critical. In blood banking, an automated system is considered critical if:

- its use 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 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.

4. Responsibility

The overall responsibility for the validation process 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 user and quality groups. 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.

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

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

5. 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.

5.1 Project change control

Before releasing an automated system and during the validation process, modification of the configuration of the automated system may be made to comply with expectations.

Any change occurring during the installation phase 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:

- hardware;
- software: including application software, operating systems, DBMS (Database Management Systems), firmware, library files, configurable packages, drivers and compilers;
- configuration files/reference tables;
- conversion programs;
- manuals (user manuals, system manuals);
- development documentation;
- training materials;
- SOPs.

5.2 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.

All proposed modifications, enhancements or additions should be assessed to determine the affect 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 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).

6. Validation process throughout automated system lifecycle

6.1 Start up

Validation should start when the decision is made to acquire a new automated system (including new information system, 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.

6.2 User Requirements Specification (URS)

A URS is required for a new automated system or significant change to an existing system (minor changes should be captured by the change control process). It is a description of what the user wants or expects from the system. It does not include any 'how' but should state clearly what is required.

The development of a URS is not an easy task and requires both expert knowledges of the business and analytical skills. It is the user's responsibility but often may only be completed

following consultation with the supplier. It should form the basis of the contract with the supplier and should be used to define the acceptance test criteria.

In the case of custom developed software the URS will form the basis for a functional specification, which describes each of the system functions necessary to meet the users requirements.

GAMP recommends that the following guidelines should be followed 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;
- both user and supplier must understand the URS; ambiguity and jargon should be avoided;
- wherever possible, the URS should distinguish between mandatory/regulatory requirements and desirable features.

6.3 System selection

System selection is based on the following considerations.

6.3.1 URS review

The URS is sent to the potential suppliers, who response should be based on the functionality of their system (Functional Specification) and how well they meet the user requirements.

6.3.2 Supplier qualification

Once the user has chosen a potential supplier, based on the URS, then their suitability must be verified.

The exact nature of the qualification will depend on:

- the user's policies for supplier qualification;
- the nature of the automated system;
- the risk assessment. (see 6.4 Risk assessment)

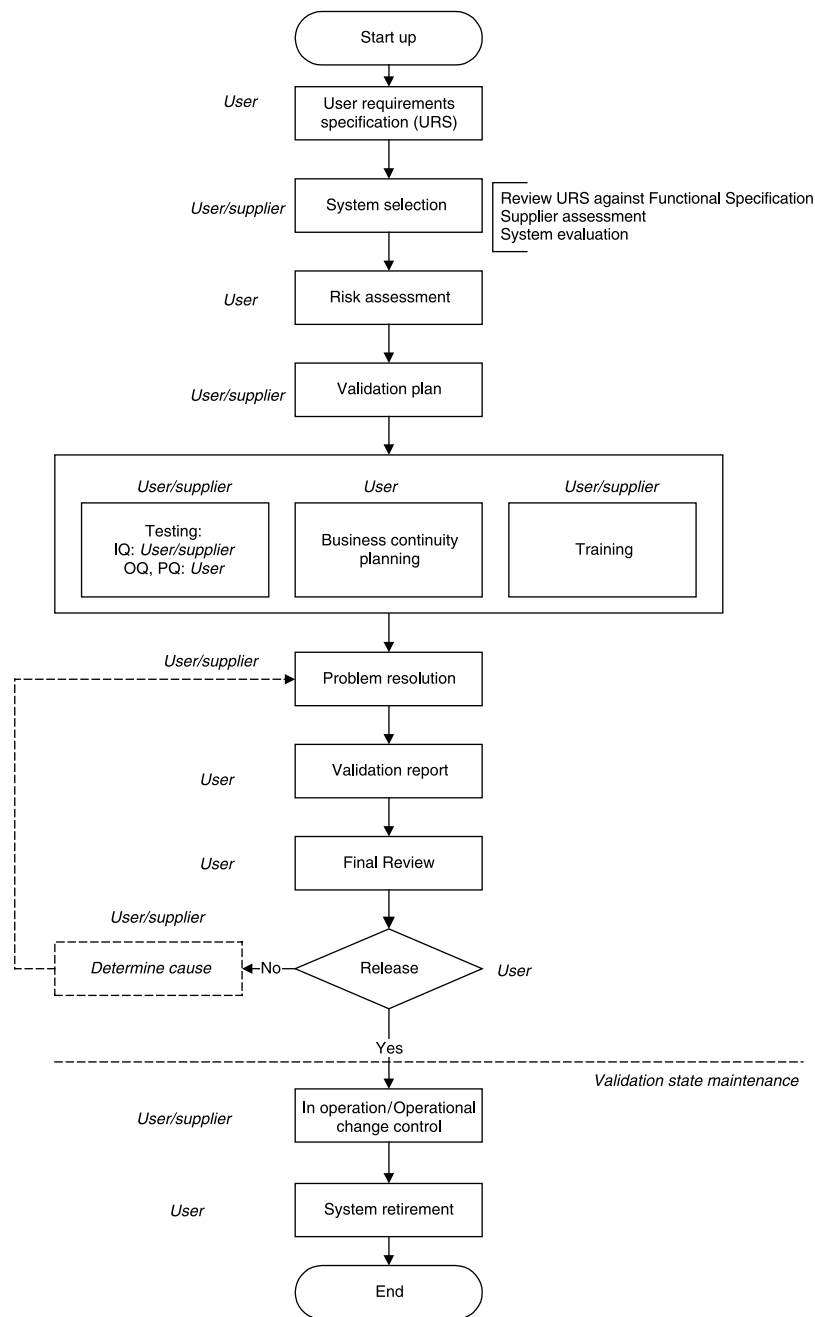
The supplier is assessed using a questionnaire/survey, an on-site audit or a combination of both. A qualified auditor or a third party can perform the audit. The audit should assess the status of the supplier's quality system. Particular attention should be given to the proposed arrangements for support and maintenance. If the supplier is an existing supplier, the results of previous audits should be reviewed and taken into account when assessing the supplier. For less critical applications assessment by questionnaire may be deemed to be sufficient.

Arrangements for the supplier audit should be formally agreed upon by the user and supplier and documented.

6.3.3 System evaluation

System evaluation consists of:

- evaluating the system against standards including GxP;
- evaluating the system against established requirements;



Responsibility of the user and supplier is attributed for each step of the validation process

Fig. 1 Validation process throughout automated system lifecycle.

- evaluating the needs of system and environment configuration;
- evaluating the requirements for installation;
- evaluating the training requirements;
- ensuring the supplier uses a recognized development methodology.

Results of the system evaluation should be presented in a report.

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

6.3.4 Financial Considerations

Financial considerations are an important element in the selection of a new automated system. The user should consider:

- One-time implementation costs such as:

- *software licensing;*
- *hardware and peripheral costs;*
- *conversion, installation, and training costs;*
- *travel and lodging expenses, etc.*
- On-going costs, such as:
 - *software support;*
 - *hardware and network maintenance;*
 - *additional staffing in technical, quality, end user areas, etc.*

6.4 Risk assessment

Risk assessment is required when a new automated system is to be implemented, changed or upgraded. It must be performed to identify critical control points, to determine the degree of testing required and to define risk mitigation plans.

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.

A risk assessment has an important place in the validation process as it can maximize testing resources through 'Better/Smarter' testing. Since it is impossible to test everything, it is best to identify the riskiest functionalities and spend proportionally more time and effort on validating these processes. It provides a set of guidelines to ensure that those modules with the highest degree of risk are focused on most heavily. And once defined, a risk assessment helps to explain the impact of a software failure, be it either functional or financial.

Many automated systems used in blood banking are considered as *configurable software packages*. A typical feature of these systems is that they permit each end-user to develop their own applications by customizing/configuring the system. Each application then becomes specific to this user 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. Again, making it impossible for the vendor to validate each different type of final system. Also, redundancy of testing for higher risk functionality is a way of providing 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 category assigned. An example of a useful categorization is in Table 1.

Next, options should be provided for risk reduction, either to mitigate and/or eliminate the risk. It may be decided that the risks in the system are so high, it should not be implemented. If it is decided to go forward with implementation, design controls, either process or product, need to be used to mitigate and/or eliminate the identified potential risks.

Table 1

High	Risks are considered to be Intolerable
Medium	Risks are Undesirable
Low	Risks are so low as to be Negligible

Mitigation generally involves creating workarounds, either with independent software or written SOPs that keep the end-user from replicating the risky system process. Documentation of the entire process must be produced, approved and controlled.

6.5 Validation plan

A 'validation plan' should be prepared after a decision is made to implement a new, or change an existing system. The level of risks is a major factor in determining the level of effort to be applied in testing and other verification and validation tasks. If the validation process encompasses only one validation study, the information normally contained in the validation plan may be included in the validation protocol. The validation plan is a historical record that is archived at the completion of the validation process. It may be revised, under change control, during the life of the validation process.

The completed validation plan shall be reviewed and approved according to the facility's quality system policies. It is recommended that the validation plan be prepared as a co-operative effort by subject matter experts.

The 'validation plan' will provide a description of the automated system, the validation activities, responsibilities, and procedures on how the validation is to be done.

User and supplier roles and responsibilities for the validation activities will be defined. The identity of authors, reviewers and approvers of the deliverables are identified in the plan. Procedures for documenting, reporting, evaluating and resolving deficiencies and defects 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 'validation protocols' will be used to produce documented evidence that the system performs as intended.

6.5.1 Validation approach

The validation approach should cover the following topics.

Scope of the validation. This involves:

- the automated system's identification;
- the context of use of the automated system;
- the processes to be employed;
- the aim of the validation.

Validation strategy. The strategy to follow for validation will depend on the 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 use and the administration of the concerned automated system. Validation activities can be performed *prospectively, retrospectively or concurrently* (see section 12 *Glossary* section for definitions).

Installation Qualification IQ, Operational Qualification OQ, and Performance Qualification PQ, classify the different validation tasks that have to be performed for ensuring the quality of the use of an automated system.

Installation Qualification (IQ). IQ shows that the system has been installed correctly. Support from the supplier is required during IQ testing. Important IQ considerations are:

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

Operational Qualification (OQ). In this phase the automated system and process operating parameters should be challenged to insure that they will result in a product that meets all defined user requirements under all anticipated conditions of manufacturing, i.e. worst case testing. OQ considerations include:

- configuration;
- process control limits monitored by the automated system;
- software operational parameters (link to the functional and design specifications ideally as provided by supplier);
- automated system operational specifications;
- process operating procedures;
- process change control;
- training;
- preventive maintenance and calibration and monitoring;
- data to prove stability and capability of the process where the automated system is used;
- evaluations for potential failure modes and worst-case conditions (risk analysis and critical control points, failure mode and effect analysis, fault tree analysis).

Performance Qualification (PQ). The objective is to demonstrate that the computerized process will consistently produce acceptable product/output under normal operating

conditions. 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 in operation;
- reconfirm acceptability of the computerized processes as established in OQ;
- reconfirm process repeatability and assure process stability when used in the field with trained operators;
- data conversion and migration to the new platform.

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

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, information technology, facilities engineering, manufacturing and others depending on the subject (laboratory, technical services, research and development, regulatory affairs, purchasing).

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

- evaluate the time and resources spent on the validation;
- define the periodicity that the validation should be performed;
- define the time when the automated system should be in operation.

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

6.5.2 Validation protocols

Validation protocols are developed 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 should be included.

6.6 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 specify who requires training, at which level they have to be trained and the documents the training is based on. The choice of the appropriate training methods will be determined based on supplier support and system complexity.

Once the documentation is established and the automated system installed, training can be performed with or without instructors, but supported with clear training instructions and concurrent documentation. The competency of the trained staff should be evaluated and documented. Operators should be able to perform the intended functions and respond in an appropriate and timely manner to all alarms, warnings and error messages.

6.7 Testing

Prior to testing, the system must be configured and frozen and a change control mechanism must be established. All documents 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 section 6.9 *Problem resolution*). The following rules for testing must be applied:

- all test results should be recorded indelibly;
- any corrections should be crossed out with a single line;
- shorthand notations such as ticks should be avoided;
- test results should be documented directly as testing occurs and should be retained – this includes screen prints, reports, queries, etc.;
- problem logs and resolution should be maintained;
- testing summaries should be established.

Test results should be reviewed and approved by a competent independent person.

6.8 Business continuity plan

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.

- A **countermeasure plan** is a preventive plan that should be prepared to reduce the risk of system failure. This can include hardware redundancy, maintenance, system monitoring and data backup procedures, training and security arrangements.
- A **disaster recovery plan** should be prepared detailing how the system will be recovered and brought back into operation.
- **Continuity action plans** should identify those critical activities that must be maintained during the period of system unavailability and specify alternative procedures to be followed during this period.

The elements of the business continuity plan should be tested during validation and be subject to periodic review and re-testing to verify their effectiveness.

6.9 Problem resolution

All problems encountered during testing should be documented. Problems will fall into two categories: validation test case failures and issues not related to testing.

Validation failures

The following tasks have to be performed:

- document all incidences of test case failure;
- investigate all failures:
 - *determine if the test case was properly written;*
 - *determine if there was user error in executing the test case;*
 - *or a system limitation;*
- document findings and resolution;
- 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.

Issues not related to testing

Issues or problems that arise should be documented, investigated and resolved before going live with a system. They are encountered when system limitations exist because of e.g. environment and resource constraints. Documenting the solution will result in historic information that will be valuable when making future decisions. Depending on how critical is the solution, a test case should be executed.

6.10 Validation report and final review

The 'validation report' presents the results of the validation activities, interpretation of the results and the conclusions drawn. If unexpected results are obtained it defines what changes will need to be made or what 'workarounds' need to be implemented 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 all documents generated during that process. 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;
- verification that data conversion is complete and accurate;
- any non-conformance was addressed through problem resolution;
- training requirements have been met;
- business continuity plans are in place.

The possible outcomes from this review are:

- release;
- conditional release;
- do not release.

If the system cannot be released or can only be conditionally released, the decision must be documented with reasons and proposed resolution.

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

6.11 Validation state maintenance

Maintaining the validated state is one of the most difficult parts of guaranteeing the usability 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:

- calibration and monitoring;
- preventive maintenance;
- training and competency;
- supplier re-qualification;
- periodic review;
- performance monitoring;
- system retirement.

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

6.11.1 Calibration and monitoring

In order for any system (not limited to automated systems) to maintain the validated state, all measuring and test equipment required by the application should be identified and calibrated.

(a) It is necessary to establish a mechanism for assuring the adequacy of the calibration and monitoring programs and ensuring that qualified personnel are available for its implementation.

(b) A calibration and monitoring plan is used to define the requirements for establishing and implementing a calibration program that includes frequency of monitoring. This will ensure that the measuring and test equipment required for any process remains calibrated to within the manufacturer's specifications or the tolerances required by the facility. The calibration and monitoring procedure must be traceable to a recognized international standard.

(c) Trending and analysis of calibration and monitoring results should be a continuous process.

(d) Calibration and monitoring intervals should be determined for each item of equipment. The intervals should be established with the intent of achieving and maintaining a desired level of accuracy and quality.

(e) The calibration status of all equipment that requires calibration should be readily available.

Record of calibration and monitoring should contain:

- item identification;
- date of last calibration and monitoring;
- due date (or usage time or frequency) for re-calibration and re-monitoring;
- the person who executed the calibration and monitoring;
- calibration certificate number (where available);
- identity of calibrators and standards used;
- results of calibration and monitoring;
- calibration and monitoring history.

(f) There should be a calibration procedure for each item type.

6.11.2 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.

(a) All equipment that requires PPM should be identified.

(b) Maintenance intervals should be determined for each item of equipment.

(c) The maintenance status of all equipment, that requires PPM, should be readily available.

Records should be maintained for all equipment and should contain:

- item identification;
- date of last maintenance;
- due date (or usage time or frequency) for maintenance;
- the person who performed the maintenance;
- PPM history;
- link to calibration and monitoring records if appropriate.

6.11.3 Training and competency

The ability of the staff to use and support an automated system correctly should be maintained. The training program

should be reassessed for any critical change in environment, process or to the automated system.

The training program should be adapted for each important staff reassignment or new 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 whole validation process.

6.11.4 Suppliers re-qualification

The ability for a supplier to maintain their activities related to an automated system has to be re-qualified on a regular basis in order to anticipate their weakness, to improve the partnership or eventually to manage the supplier and/or automation system changes.

The periodicity and the detail of the re-qualification process depends on the level of risk from using the automated system. Re-qualification 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 re-qualification is not limited to the audit, but also concerns the follow-up to postaudit findings.

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

6.11.5 Periodic review

Periodic review aims to establish that the system and validation documentation is complete, current and accurate.

Periodic review should be planned and scheduled. It should consider:

- validation documents for the system;
- documentation for using and supporting the system (SOPs, operational plans, related records);
- GxP regulations;
- system maintenance, calibration and monitoring, change and incident logs;
- any prior audit reports;
- change in environment, process or business requirements, legislation or accepted best practices;
- personnel;
- supplier's contract review (including problem handling, downtime, etc.).

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

- the relevant results obtained from the review;
- deviations or problems found;
- required remedial work;

- the ratification of the continued acceptability for the system use.

Identified actions should be prioritized and planned.

6.11.6 Performance monitoring

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

Critical system conditions should be monitored with suitable monitoring tools at appropriate time intervals. The monitoring plan should state acceptable system parameters, 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, a backup plan may need to be implemented to keep the system operating (see section 6.8 *Business continuity plan*).

6.11.7 System retirement

At the end of 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;
- the data should be archived such that it can be retrieved and read;
- an archive report should be generated describing the archive approach and listing the documents, raw data and electronic records archived;
- it should be possible to retrieve the data independently of the original system;
- the data should be retained as required by the regulations and company policy.

7. Security

Security policies should be developed for defining the rules and guidance regarding use and access to critical information.

7.1 User access policies

User access policies should be developed that require unique identification codes for each user, periodic password change, prohibition of sharing passwords and mechanisms to ensure users are added to and deleted from the system as appropriate and when authorized. Any deviations and/or modifications will be documented and approved.

Appropriate measures should be taken against unauthorized input, deletion, or modification of critical data.

7.2 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 licences;
- external automated systems.

Procedures should describe how the policies are implemented.

8. Back-up and recovery

To guarantee the availability of stored electronic data, back-ups should be made periodically (and when any important software system change occurs) for data required to reconstruct GxP relevant documentation. This also applies to any system (software, environment configuration including the operating system) that manages the data.

- The back-up process should guarantee data integrity; each back-up should be checked to ensure that it is error free;
- The back-up process, the number of backup copies, the frequency of back-up, the back-up verification process and the restore process should be specified and documented;
- The back-up copies should be stored in a secure place and in an appropriate environment (protected from fire, water and others hazards) that guarantees the quality of the storage medium; it should be in a location separate from the system;
- Copies of the storage medium should be made before the expected life of the storage medium has expired;
- Each back-up medium should be clearly identified;
- A log of software back-ups should be maintained;
- The method of restoring and control should be specified for when data recovery is required.

9. 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 off-line 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 wilful or accidental damage;
- storage facilities and environment conditions should minimize the degradation of record storage media that could result in the loss of data;
- 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.

10. References and Reading List

- 1 GAMP – Guide for Validation of Automated Systems. *GAMP Forum, Version 4. ISPE*. December, 2001
- 2 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
- 3 Validation Master Plan Installation and Operational Qualification Non-Sterile Process Validation Cleaning Validation. PIC/S – Pharmaceutical Inspection Convention & Pharmaceutical Inspection Co-Operation Scheme. <http://www.picscheme.org/docs/pdf/validate.pdf>. August, 2001
- 4 Good Practices for computerised systems in regulated 'GxP' environments. PIC/S – Pharmaceutical Inspection Convention & Pharmaceutical Inspection Co-Operation Scheme. Draft version. <http://www.picscheme.org/docs/pdf/computerised.pdf>. January, 2002
- 5 21 CFR Part 11 Electronic Records, Electronic Signature Final Rule. Department of Health and Human Services – Food and Drug Administration. http://www.fda.gov/ora/compliance_ref/part11/FRs/background/pt11finr.pdf. March, 1997
- 6 Medical Device Quality Manual System-7. Equipment and Calibration. U.S. Food and Drug Administration – Center for Devices and Radiological Health. <http://www.fda.gov/cdrh/qs/intro.html>. January, 1997
- 7 Mullendore B, Chapman KG: Proposed Validation Standard VS-2 Computer-Related System Validation. *Journal of Validation Technology* 2003; 7 (3).
- 8 Risk Assessment Program Quality Assurance Plan. *Environmental Management and Enrichment Facilities*. Lockheed Martin Energy Systems, Inc, <http://risk.lsd.ornl.gov/homepage/tm/tm117.pdf>. November, 1997
- 9 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
- 10 Medical Device Quality Manual System-4. Process Validation. U.S. Food and Drug Administration – Center for Devices and

- Radiological Health. <http://www.fda.gov/cdrh/qsr/intro.html>. January, 1997
- 11 Medical Device Quality Manual System-5. Personnel and Training. U.S. Food and Drug Administration – Center for Devices and Radiological Health. <http://www.fda.gov/cdrh/qsr/intro.html>. January, 1997
 - 12 Medical Device Quality Manual System-15. Complaints. U.S. Food and Drug Administration – Center for Devices and Radiological Health. <http://www.fda.gov/cdrh/qsr/intro.html>. January, 1997
 - 13 GLP: Consensus Document the Application of the Principles of GLP to Computerised Systems, Environment Monograph no. 116 – OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring – no. 10. Organisation for Economic Co-Operation and Development. <http://www.iph.fgov.be/GLP/home.html>. 1995
 - 14 PIC/S GMP: Guide for Active Pharmaceutical Ingredients. PIC/S – Pharmaceutical Inspection Convention & Pharmaceutical Inspection Co-Operation Scheme. <http://www.picscheme.org/docs/pdf/gmpapi.pdf>. August, 2001
 - 15 ISO/IEC.14598-4:1999 Software engineering – Product Evaluation Part 4: Process for Acquirers. International Standardization Organisation. 1999
 - 16 GAMP – Good Practice Guide. Calibration Management. ISPE. 2002
 - 17 Good Practice and Compliancy for Electronic Records and Signatures Part 1-Good Electronic Records Management (GERM). ISPE, PDA: 2002
 - 18 Good Practice and Compliancy for Electronic Records and Signatures Part 2-Complying with 21 CFR, Part 11 Electronic Records and Electronic Signatures. ISPE: PDA. 2001
 - 19 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. <http://www.fda.gov/cdrh/ode/57.html>. May, 1998
 - 20 Glossary of computerised System and Software Development Terminology. Inspection references. Inspection Guides. U.S. Food and Drug Administration Office of Regulatory Affairs. http://www.fda.gov/ora/inspect_ref/igs/gloss.html. August, 1995
 - 21 GLP-Guidelines for the Validation of Computerised Systems. Working Group Information Technology (AGIT), Version 1. <http://www.glp.admin.ch/legis/val1-0.pdf>. June, 2000
 - 22 Validation in Blood Establishments and Transfusion Services. AABB Press. 1996
 - 23 ISO 9001. 2000 Quality management systems – requirements. International Standardization Organisation. 2000

11. Acronyms

GAMP: Good Automated Manufacturing Practice
GCP: Good Clinical Practice
GLP: Good Laboratory Practice
GMP: Good Manufacturing Practice
GxP: Good 'x' Practice, where 'x' one of:

- Clinical
- Distribution
- Laboratory
- Manufacturing

IQ: Installation Qualification

OQ: Operational Qualification

PPM: Planned Preventive Maintenance

PQ: Performance Qualification

QA: Quality Assurance

QMS: Quality Management System

SOP: Standard Operating Procedure

URS: User Requirement Specification

UPS: Uninterruptible Power Supply

12. 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 laboratory or manufacturing database systems. The automated system consists of the hardware, software and network components, together with the controlled functions and associated documentation.

Calibration: The set of operations, which establish, under specified conditions, the relationship between values indicated by a measuring instrument or measuring system, or values represented by a material measure and the corresponding known values of a reference standard.

Certificates of calibration: Document signed by qualified authorities that testifies that a system's qualification, calibration, validation or revalidation has been performed appropriately and that the results are acceptable.

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 program and also for all or part of the data necessary for the execution of the program; executes user-written or user-designated programs; performs user-designated data manipulation, including arithmetic operations and logic operations; and that can execute programs that modify themselves during their execution. A computer system may be a stand-alone unit or may consist of several interconnected units.

Computerized system: Includes hardware, software, peripheral devices, personnel and documentation, e.g. manuals and Standard Operating Procedures.

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 specifications: 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 utilizing 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.

Software design specifications: Description of logical and physical structures of the program, 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 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): Provides a 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 defines also 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.

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 protocols: Prospective experimental 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 conducted when there is no possibility to complete a validation program 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 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 1: Documentation

Documentation is an important element of the validation process. The following documents typically required to provide an audit trail and assure the quality of the validation process including the maintenance of the validation state.

Steps of the validation process	Type of documents	Supplied by
User requirements specification	<i>User Requirements Specification (URS)</i>	User
System selection	<i>Installation requirements</i> <i>Functional specifications*</i> <i>Hardware design specifications*</i> <i>Software design specifications*</i> <i>Engineering diagrams*</i> <i>Manual/user guides</i> <i>Supplier questionnaire/survey</i> <i>Supplier audit report</i> <i>System evaluation report</i>	Supplier User
Risk assessment	<i>Risk analysis</i>	User
Validation plan	<i>Validation plan</i> <i>Validation protocol</i>	User
Training	<i>Training plan</i> <i>Documentation of training</i> <i>Training material</i>	User and Supplier
Testing (IQ)	<i>Test results</i>	User and Supplier
Testing (OQ, PQ)	<i>Test results</i>	User
Business continuity plan	<i>Countermeasures plans</i> <i>Disaster recovery plans</i> <i>Continuity action plans</i>	User
Problem resolution	<i>Problem resolution records</i>	User
Validation report	<i>Validation report</i>	User
In operation	<i>Maintenance, calibration and monitoring plans and records</i> <i>Periodic audit/review plans and reports</i> <i>Change control and incident records</i>	User
System retirement	<i>System retirement plan and report</i>	User

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

SOPs	Supplied by
<ul style="list-style-type: none"> • Use of the automated system • Support activities • Backup and recovery • Archiving and record retention • Change control • Security management • Periodic review • Business continuity • System retirement • Training • Maintenance, Calibration, Monitoring 	User

Appendix 2: Classification of automated systems

GAMP Guide for Validation of Automated Systems [1] and the PIC/S Good Practices for computerized systems in regulated 'GxP' environments [4] categorize automated systems and the applied tasks as follows.

Category 1: Operating system

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).

Category 2: Firmware

Firmware is the combination of a hardware device, computer instructions and data. The software cannot be modified during processing by the computer. The name, version and any configuration or calibration should be documented and verified during Installation Qualification (IQ). Functionality should be tested during the Operational Qualification (OQ).

Category 3: Standard software packages

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: Configurable software package

Configurable software packages provide standard interfaces and functions that enable 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 (Bespoke) Software

Custom systems are developed to meet 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 the Performance Qualification (PQ).

Table 3 Example of classification of automated systems used in blood banking

Automated system	Automated system Categories
Air handling systems	4, 2
Alarm system	4, 2
Apheresis machines	4
Automated component processing system	4, 2
Autonomous computer system with critical information (e.g. laptop)	5, 4, 3
Balance/mixer	4, 2
Barcode reader	4
Blood pressure automated system	2
Blood product storage devices	4, 2
Centrifuge	4, 2
Computer system (including emulator)	5, 4, 3
DBMS (Database Management System)	1
ECG machine	2
Electronic archive system	5, 4, 3
Electricity backup system, UPS	4, 2
Electronic balance	2
Electronic thermometer	4, 2
Fast freezer	4, 2
Hb meter	2
Heat sealer	2
Incubator	4
Irradiator	4, 3, 2
Laboratory automated system	4
LIMS (Laboratory Information Management System)	4
Network	2
Network device	4
Printer	4
Operating system	1
Software application	5, 4, 3
Tube docking system	2

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