

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

Persons who have participated in the writing of this document:

Janet Sampson, Welsh Blood Service, Wales (Co-Chair)
Robin Nozick, R. F. Nozick and Associates, USA (Co-Chair)
Paul Ashford, ICCBBA, USA
Wolfgang Boecker, Fresenius Kabi Deutschland GmbH, Germany
Pia Bruce, Finnish Red Cross Blood Service, Finland
Dr Patrick Coghlan, Australian Red Cross Blood Service, Australia
John Davies, Sweden
Rodeina Davis, Blood Center of Wisconsin, Milwaukee, USA
Pat Distler, ICCBBA, USA
Thomas Dullaart, Sanquin, The Netherlands
Peggy Dunn, Puget Sound Center, Seattle, USA
Lone Espensen, Odense University Hospital, Denmark
Oluwafemi Faseemo, Christus Spohn Health System, Corpus Christi, Texas, USA
Simon Fournier, Héma-Québec, Montréal, Canada
Shankar Goudar, Carter BloodCare, Bedford, Texas, USA
Sandy Hedberg, SoftwareCPR, USA
Susan Hudson, American Red Cross, Washington D.C., USA
Gerhard Jirsa, Austrian Red Cross Blood Donation Center for Vienna, Lower Austria and Burgenland, Vienna, Austria
Bonnie Lupo, Continuum Health Partners, New York, USA
Sue McDonnell, Irish Blood Transfusion Service, Ireland

The publication of version 2 of these guidelines reflects the enormous contribution made by the International Society of Blood Transfusion Working Party on Information Technology Validation Task Force members listed above whose contributions covered both authorship and reviewing of material. In addition it is appropriate to recognise the contribution made by the following colleagues in producing version 1 of the guidelines published in 2003:

Mike Clark, England
Christian Desaint, France
Carlos Izaguirre, Canada
Angelika Kawaters, Germany
Charles Munk, Switzerland

Introduction

The ISBT Guidelines for Validation and Maintaining the Validation State of Automated Systems in Blood Banking were first published in 2003 and have since been recognized by blood establishments and suppliers of automated systems as a useful document in promoting a standardized approach to the complexities of validation projects for critical computer systems and equipment in blood establishments.

Version 2 of the guidelines, replacing the previous version, is renamed ISBT Guidelines for Validation of Automated Systems in Blood Establishments, and has been written to take account of changes within the regulatory environment and developments in validation methodology, and to ensure that the document remains relevant to the validation challenges faced by blood establishments today and for those they are likely to face in the future.

The comprehensive re-write of the guidelines expands the scope of validation activities covered and takes account of, and reflects, the recent developments of ICH Q8, ICH Q9, ICH Q10, GAMP[®] 5 and PIC/S. Specific additions include the following: a clearer definition of validation and its relationship to an organisation's Quality Management System (QMS); the effect of risk assessment on what and how much validation is necessary; sections on validating Data Migration software and Network Infrastructure; performing Supplementary Qualifications; the use of validation platforms; and validating software patches.

The blood establishment bears the responsibility for the regulatory compliance of the automated/computerized systems used. Full validation of the computerized system is required for systems that are critical to product quality (information management, storage, tools for operational decision-making, and control). These guidelines do not advocate a particular validation methodology but do promote the Quality Risk Management approach to validation advocated by GAMP[®] 5 and ICH Q9, a life cycle approach within the QMS, and the use of risk assessments to define the validation strategy for critical systems. 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 guidelines should be adapted to each blood establishment's needs considering:

- the size and type of the organisation;
- the impact of risk in blood establishments;
- the need to have reliable automation systems;
- the diversity of activities taking place in blood establishments;
- the evolution of regulations and the national legislation;
- the possibility to leverage the supplier documentation and knowledge; and
- the resources needed to implement a validation process.

It is important that the approach to validation used by a blood establishment should allow provision for the process to be scalable to the functionality of the system, e.g. the validation of a centrifuge is less complex than that for a bespoke blood management system. The guidelines include an updated appendix which lists common blood establishment equipment and the recommended approach to their validation.

The following were chosen as the main references for the version 2 of the ISBT guidelines:

- GAMP[®]5 A Risk-based Approach to Compliant GxP Computerized Systems [1];
- Guidance for Industry ICH Q8 Pharmaceutical Development [7];
- Guidance for Industry ICH Q9 Quality Risk Management [8];
- Guidance for Industry ICH Q10 Pharmaceutical Quality System [9];
- 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 Computerised Systems in Regulated 'GxP' Environments Guidelines [4].

The benefits of validation have remained as follows:

- 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.

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 objective of validation 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.

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, i.e. users/technical reps/validation/QA/IT professionals;
- Risk assessment;
- Cost efficiency.

Validation is a complex process. The skillsets 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.

Clearly, the process is easier to perform with qualified staff and where validation processes are already established and embedded into the organization.

For those organisations who are about to adopt validation practices and who 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 is performed before systems are used operationally.
- Use should be made, where possible, of supplier system and test documentation to reduce the blood establishment's qualification effort.
- When performing retrospective validation of equipment it is worth considering whether the existing QMS documentation may be sufficient to comply with the minimum regulatory requirements of demonstrating control and approval via, for example, specification, risk assessments, qualification, traceability and validation report.

Acknowledgements

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

American Red Cross, Washington DC, USA
Australian Red Cross Blood Service, Australia
Austrian Red Cross, Blood Donation Center for Vienna, Lower Austria and Burgenland, Vienna, Austria
Carter BloodCare, Bedford, Texas, USA
Christus Spohn Health System, Corpus Christi, Texas, USA
Continuum Health Partners, New York, USA
Finnish Red Cross Blood Service, Finland
Fresenius Kabi Deutschland GmbH, Germany
Héma-Québec, Montréal, Canada
ICCBBA, USA
Irish Blood Transfusion Service, Ireland
Odense University Hospital, Denmark
Puget Sound Center, Seattle, USA
R. F. Nozick and Associates, USA
Sanquin, The Netherlands
SoftwareCPR, USA
Blood Centre of Wisconsin, USA
Welsh Blood Service, Wales

Conflicts of interest

Robin Nozick declares that she is an Executive of a company which performs Validation and other Quality Management Services for Clinical Laboratories and Transfusion Services. All other authors have declared no conflicts of interest.

Contents

Introduction	i
Acknowledgements	ii
1. Overview	1
2. Purpose	1
3. Scope	1
4. Responsibility	1
5. Change control	2
5.1 Project change control	2
5.2 Operational change control	2
5.3 System inventory	2
6. Validation process throughout automated system lifecycle	3
6.1 Start up of validation	4
6.2 User Requirements Specification (URS)	4
6.3 System selection	4
6.3.1 URS review	4
6.3.2 Supplier qualification	4
6.3.3 System evaluation	4
6.3.4 Financial considerations	5
6.4 Risk assessment	5
6.5 Validation plan	5
6.5.1 Validation approach and content of the validation plan	6
6.5.2 Validation protocols	7
6.6 Data migration	7
6.6.1 Plan	8
6.6.2 Execute and report	8
6.6.3 Perform migration verification	8
6.7 Infrastructure qualification	9
6.7.1 Servers and hosts	9
6.7.2 Network infrastructure	9
6.7.3 Clients	10
6.8 Training	10
6.9 Testing	10
6.10 Business continuity plan	10
6.11 Problem resolution	11
6.12 Validation report and final review	11
6.13 Handover (go-live) process	11
6.14 Validation state maintenance	11
6.14.1 Calibration and monitoring	12
6.14.2 Preventative maintenance	12
6.14.3 Software patches/service packs installation	12
6.14.4 Training and competency	12
6.14.5 Suppliers re-qualification	13
6.14.6 Periodic review	13
6.14.7 Performance monitoring	13
6.14.8 System retirement	13
7. Security	13
7.1 User access policies	14
7.2 System access policies	14
8. Back-up and recovery	14
9. Archive and record retention	14
10. References	14
11. Reading list	15
12. Acronyms	15
13. Glossary	16
Appendix 1 Documentation	18
Appendix 2 Classification of automated systems	19

ISBT Guidelines for Validation of Automated Systems in Blood Establishments

1. Overview

Every blood banking organization must have a Quality Management System. This should include a section on validation (e.g. Validation Master Plan or Validation Policy) that describes the organisation'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 organisation's validation policy should comply with the regulatory requirements applicable in the country of use.

These guidelines address the validation needs for automated systems, i.e. 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, maintenance and calibration.

Validation requires a structured approach. The approach normally used for automated systems makes use of the methodologies developed initially to manage software development, based on the concept of a computer system life cycle.

A computerized system life cycle includes phases from the initial concept of the system, through project and operation phases, 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, assurance of quality and fitness for intended 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. According to GAMP[®] 5, separate computer system validation should be avoided in

the case of automated manufacturing equipment. Instead, the system specification and verification should be part of the complete automated equipment validation ensuring compliance and fitness for intended use. Additional validation in the blood centre, at a minimum, should include provision of a written description of the system elements and their functions, and on-line performance testing of the system under at least limiting and boundary conditions. A record should be kept of the validation testing.

2. 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 organisations involved in blood collection, testing, processing, distribution and transfusion.

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

3. Scope

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, storage, 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.

4. 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 in an adequate way.

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;
- quality assessments of third-party suppliers;
- problem resolution;
- identification and provision 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);
- 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.

Change should be initiated and controlled by the process owner.

5.1 Project change control

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

Any change occurring during the implementation 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;
- data migration files and programs;
- manuals (user manuals, system manuals);
- development documentation;
- validation documentation;
- training materials;
- SOPs.

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

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. Operational change management should continue until system retirement.

All proposed modifications, enhancements or additions should be reviewed and 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). Where required, SOPs 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 modifications, emergency or repair changes, or for workarounds provided sometimes by the software vendor.

It is the responsibility of the system process owner to ensure that a change control process and procedures are in place that support changes to the system.

It is the responsibility of Quality Assurance to ensure SOPs are followed.

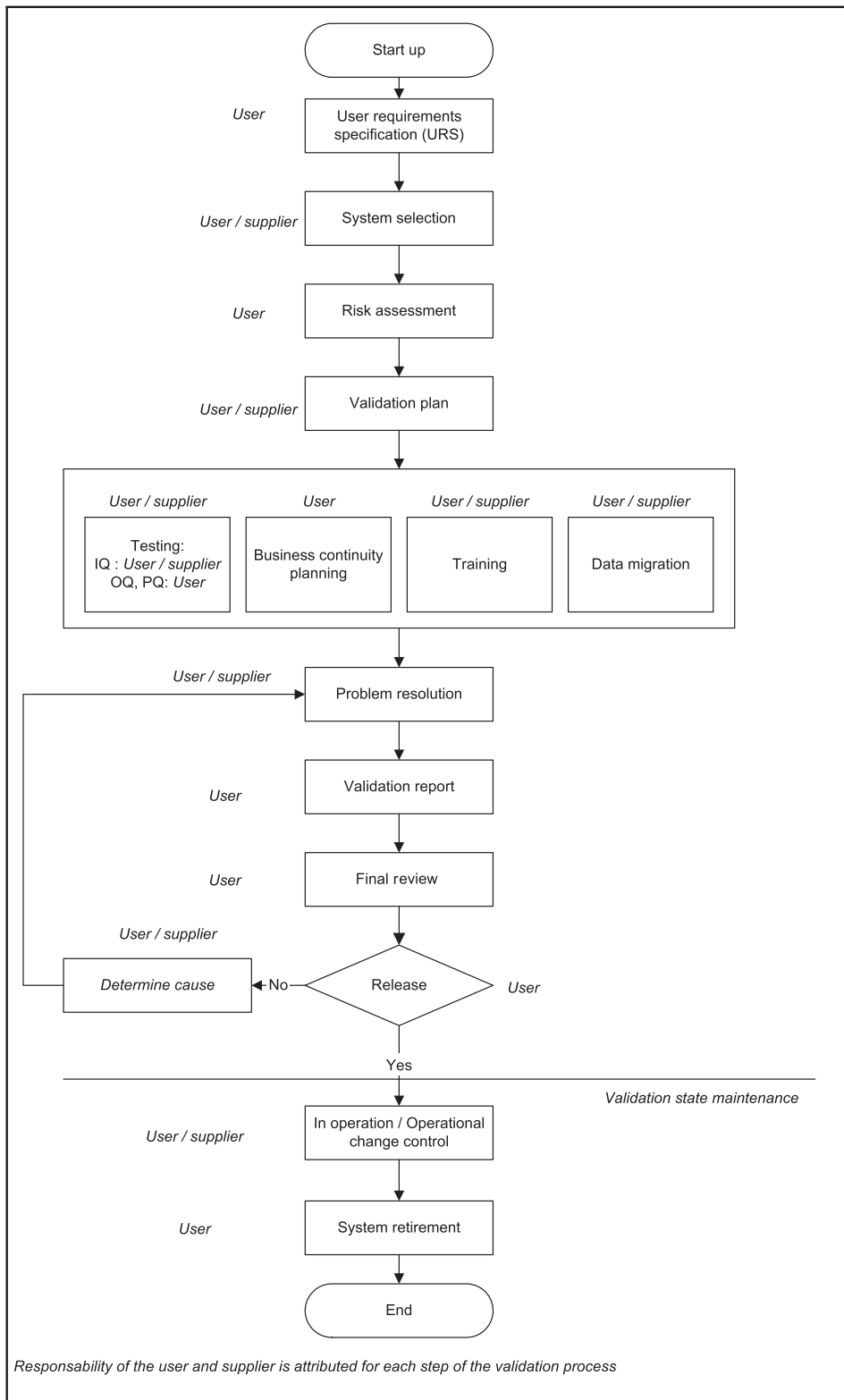
It is the responsibility of each member of the change team to execute the assigned activities accurately and completely.

5.3 System inventory

A system inventory should be maintained which specifies for each critical system :

- the owner of the system
- its validation status
- date when due for periodic review/re-validation.

6. Validation process throughout automated system lifecycle



6.1 Start up of validation

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

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). However, it does not include any 'how' but should state clearly 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 knowledges 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 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 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 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;
- Information security requirements should be included.

6.3 System selection

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

6.3.1 URS review

The URS is sent to potential suppliers as a request for 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 FS's are compared with the URS in order to identify suppliers and systems that may qualify.

6.3.2 Supplier qualification

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

The exact nature of the qualification will depend on:

- the user's policies for supplier qualification;
- the GMP requirements specified in the URS
- the nature of the automated system;
- the risk assessment. (see Section 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 the supplier's procedures for development, support, maintenance and distribution of updates. 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 regulations and standards including GxP;
- evaluating the system against established user requirements;
- evaluating the needs of system and environment configuration;
- evaluating the requirements for installation;
- evaluating the training requirements;
- evaluating the technological standard of the system, i.e. future proofing and the road-map of the future development;
- ensuring the supplier uses a recognised 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.

6.3.4 Financial considerations

Financial considerations are 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;
 - travel and lodging expenses, etc.
- On-going costs, such as:
 - software support;
 - hardware and network maintenance;
 - archiving of historic data and records;
 - frequency of anticipated software updates and system upgrades and the amount of revalidating involved;
 - additional staffing in technical, quality, end user areas etc.
- Retirement costs.

6.4 Risk assessment

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

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. 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 *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. 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 category assigned. An example of a useful categorization is in the following table.

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

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, controls, either process or product, need to be used to mitigate and/or eliminate the identified potential risks. Mitigation generally involves creating workarounds, either with independent software or written SOPs that prevent the end-user from replicating the risk identified 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. It is recommended that the validation plan be prepared as a co-operative effort by subject matter experts. 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 testing 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 validation plan will provide a description of the automated system, the validation activities, responsibilities,

procedures, how the validation is to be done and expected outcomes together with the acceptance requirements.

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 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 will be used to produce documented evidence that the system performs as intended.

6.5.1 Validation approach and content of the validation plan

The validation approach should cover the following topics that are included in the validation plan.

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

Quality risk management. Quality risk management should involve an initial risk 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 the administration of the concerned automated system. The amount, type and results of supplier testing may be used to focus and decide the amount of testing needed during the validation efforts.

Validation strategy should define which activities may be performed *prospectively, retrospectively or concurrently* (see Section 13, Glossary for definitions). 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 for ensuring the quality of the use of an automated system.

Installation Qualification. 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, 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. 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;
- 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);
- backup and recovery;
- system access and security.

Performance Qualification. 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;
- 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 migration to the new platform.

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 the 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 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, IT 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 spent on the validation;
- define the timeline over which 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 (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.

6.5.2 Validation protocols

Validation testing is often 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.

6.6 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 a single or multiple system. Data migration may vary in scope, complexity and risk, and should not be underestimated. The data migration process should be managed according to a specific plan and requirements described in a data migration plan.

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 but not be limited to: migration scope; roles and responsibilities; requirements and deliverables; risk analysis; configuration management strategy; software tools and strategies for ensuring compliance and fitness for intended use; data quality assessment; data mapping; data transformation rules; migration steps; data verification

strategy and acceptance criteria; system transition plan; and rollback strategy.

6.6.1 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 data is usable and that its context value remains.

For a successful migration, it is of vital importance that there is a good understanding of the data which 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. Where applicable, documented decisions should be made to cleanse the data.

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 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 on 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.

Once the data is transferred it must be verified. Execution trials should be performed several times until they meet the success criteria that have been set.

6.6.2 Execute and report

Once the data migration plan is written and approved, migration test runs should be performed in a test environment. To achieve 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.

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;
- 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 is accurately translated and completed, the integral end to end data migration process, as described in the data migration plan, can be performed in the production environment.

6.6.3 Perform migration verification

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 which 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 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 to prevent the use of redundant/incorrect data.

6.7 Infrastructure qualification

A prerequisite to ensure 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, i.e., GxP application runs in an environment which is continuously maintained and in control.

Normally the infrastructure is qualified with an IQ and sometimes OQ. The PQ of the infrastructure is *per se* performed during the validation performed on every application for its intended use.

The infrastructure can be divided into parts as follows:

- servers and hosts including operating systems and database engines;
- internal network infrastructure; switches, routers, cabling and network monitoring tools, scheduling tools etc. within the organization;
- user interfaces (clients); workstations, laptops including web access tools etc;
- external interfaces, networks and security components.

According to GAMP[®]5, 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.

6.7.1 Servers and hosts

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

(a) Requirements Specification (URS/FS) should:

- specify the functional requirements for the host machine and its operating system and utilities.

(b) Design Specification should:

- specify the actual configuration and setup of the equipment, operating system and utilities that make up the host machine.

(c) Installation Qualification should:

- capture the installation of the host, if serial number and model were defined they 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.

(d) Operational Qualification should:

- include at a minimum: backup and recovery, data archival and retrieval, security, system instruction manual verification, start-up and shutdown, uninterruptible power supply, communication loss and recovery, any system redundancy such as mirrored drives, secondary systems failover systems, etc.

6.7.2 Network infrastructure

The network infrastructure can be defined as the transportation and communication systems. Testing of the WAN and 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.

(a) Requirements Specification (URS/FS) should:

- specify the functional requirements for the major components of the WAN/LAN infrastructure;
- specify the required redundancy of the infrastructure.

(b) 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, network operating systems. WAN/LAN interfaces are included; other components such as cabling, power supplies, interface cards should also be captured.

(c) Installation Qualification should:

- capture the physical installation of the major components; if serial number and model were defined it they should be included;
- include the documentation of software on standalone switches and routers.

(d) 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. Testing of networks will need to be a team effort since many applications are part of the

network and integration with each other is very important.

(e) Performance Qualification:

- A separate PQ is not expected for infrastructure as the PQ of the infrastructure is *per se* included in the OQ and PQ of the application(s) using the infrastructure.

6.7.3 Clients

Where the Administrator access rights to the clients cannot be disabled for users they remain under the direct control of the users themselves. It is typically difficult to demonstrate a state of control in the workstation environment. It is possible to initially qualify and document the workstation, however, it produces a challenge to maintain the controlled state. The clients should be controlled via policies, procedures, CD-images, and audits. System upgrades require updated documentation and possible retesting.

(a) User Requirements Specification should:

- specify the functional requirements for the type of client workstations and laptops;
- document the organization's standard type of clients and the minimum hardware requirements as well as the current operating system, including patches, upgrades and software to be used.

(b) Installation Qualification should:

- record system information in accordance with established procedures, e.g. using a form. When a client is installed or modified a qualified individual should perform the tasks and complete the form.

(c) Operational Qualification should:

- for applications running on the clients, test and document that the application operates according to its intended use in the client/server environment.

(d) Performance Qualification:

- a separate PQ is not expected for clients as the PQ of the clients is *per se* included in the OQ and PQ of the application(s) running on the clients.

6.8 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 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.

6.9 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 Section 6.11, 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, initialled and dated – 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 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.

6.10 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 and staff must be trained on a regular basis.
- Continuity action plans should identify those critical activities that must be maintained during the period of system unavailability and document alternative processes 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. Top management has to be informed about the impact of this plan.

6.11 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 incidents to determine:
 - if the test case was properly written;
 - if there was user error in executing the test case;
 - if there was a specification error;
 - if there is 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. 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 such things as environment and resource constraints. Documenting the solution will provide historic information that will be valuable when making future decisions. Depending on how critical the solution is, a test case should be executed. A risk assessment based approach should be used.

6.12 Validation report and final review

The validation report presents the results of the validation activities, including data migration, interpretation of the results and the conclusions drawn. If unexpected results 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 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;
- data migration is complete and accurate;
- any non-conformance was addressed through problem solving;

- training requirements have been met;
- a business continuity plan is in place.

The possible outcomes from this review are:

- release;
- conditional release;
- 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.

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

6.13 Handover (go-live) process

Transfer of responsibility of an automated system from project to operation is needed once the system is ready to go-live. The handover process scope, period, acceptance criteria and plan (checklist) should be established beforehand. The handover activities performed should be described and approved paying special attention to the transfer of open issues and incomplete activities or documentation. A period of monitoring the system after go-live may be needed and a rollback strategy defined for serious problems emerging. The formal acceptance of the automated system and controlled transfer into the live operational environment should be documented.

6.14 Validation state maintenance

Maintaining the validated state is one of the most difficult activities of guaranteeing the regulatory compliance and fitness of 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:

- calibration and monitoring;
- preventive maintenance;
- incident management;
- software patches/service packs installation;
- 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.

6.14.1 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 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.

The 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;
 - 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.

6.14.2 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.

6.14.3 Software patches/service packs installation

A patch is a piece of code added to software in order to fix a bug, especially as a temporary correction between two releases. This can also include changing the user interface and improving usability and performance. Though meant to fix problems, a poorly designed patch can sometimes introduce more problems. For this reason, it is very important that the same change control procedures are followed as when an entire automated device is installed. 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. In order to determine the scope of the needed validation, an impact analysis should be performed which includes making the following assessment:

- what programming has been modified and is included in the patch/service pack?
- will this change have an impact on processes that people perform?
- what is the risk if this change does not work?

The answers to all of these questions help to determine the need for IQ, OQ, and/or PQ.

If the patch causes changes to working practices and/or processes then training people for the new processes must be done to ensure personnel perform the entire process competently. PQ and training ensure changes made are understood by anyone impacted.

When automated system vendors release a patch or service pack it is expected that they inform customers about what has been fixed or added to the software and what the impact is on the system. Normally the vendor does this by producing Release Notes, an Update Manual or Service Pack Notes that accompany the patch or service pack. Using this information, the end user should be able to answer the questions raised above. If the vendor does not disclose the changes made it is very important that documentation of the changes is provided in order to minimize the amount of validation needed and maximize the knowledge of the end user.

6.14.4 Training and competency

The ability of 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 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.

6.14.5 Suppliers re-qualification

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

The frequency 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 of post-audit 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.

6.14.6 Periodic review

Periodic review aims to establish that the system and validation documentation remains 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;
- the incremental effect of changes;
- system maintenance, calibration and monitoring, incident logs;
- any prior audit reports;
- change in environment, process or business requirements, legislation or accepted best practices;
- personnel;
- supplier's contract reviews (including problem handling, downtime, third party policy, etc.).

A report of the review process should be prepared 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 prioritised and planned. A risk assessment based approach should be used.

6.14.7 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 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, a back-up plan may need to be implemented to keep the system operating (see Section 6.10, Business continuity plan).

6.14.8 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, 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 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. It could be performed through the Guidelines on Information Security from ISBT [6].

7.1 User access policies

User access policies should be developed requiring 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 authorised. Any deviations and/or modifications will be documented and approved.

Appropriate measures should be taken against unauthorised 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 unauthorised 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 verified to ensure that it is error free;
- the back-up process, the number of back-up 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 and complies with confidentiality and privacy regulations; it should be in a location separate from the system;
- 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 in the event when data recovery is required;
- the data recovery process should be validated.

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 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;
- hardware needed to read these media has to be archived.

10. References

- 1 GAMP® 5 A Risk-based Approach to Compliant GxP Computerized Systems. ISPE. 2008. ISBN 1-931879-61-3.
- 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 and Pharmaceutical Inspection Co-Operation Scheme. <http://www.picscheme.org/publis/recommendations/PI%20006-3%20Recommendation%20on%20Validation%20Master%20Plan.pdf>. 25 September 2007.
- 4 Good Practices for Computerised Systems in Regulated "GxP" Environments. PIC/S - Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme. PI 011-3 <http://www.picscheme.org/publis/recommendations/PI%20011-3%20Recommendation%20on%20Computerised%20Systems.pdf>. 25 September 2007.
- 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 ISBT Guidelines for Information Security in Transfusion Medicine, Volume 91 Supplement 1 Vox Sanguinis. July 2006.
 - 7 Guidance for Industry ICH Q8 Pharmaceutical Development. U.S. Department of Health and Human Services Food and Drug Administration. <http://www.fda.gov/CbER/gdlns/ichq8pharm.pdf>. May 2006
 - 8 Guidance for Industry ICH Q9 Quality Risk Management. U.S. Department of Health and Human Services Food and Drug Administration. <http://www.fda.gov/cder/guidance/7153fnl.pdf>. January 2006.
 - 9 Guidance for Industry ICH Q10 Pharmaceutical Quality System. U.S. Department of Health and Human Services Food and Drug Administration. <http://www.fda.gov/cder/guidance/8515fnl.pdf>.
 11. Reading List April 2009.

11. Reading list

- 10 Medical Device Quality Systems Manual - 7. Equipment and Calibration. U.S. Food and Drug Administration - Center for Devices and Radiological Health. <http://www.fda.gov/cdrh/qsr/07.html>. January 1997.
- 11 Proposed Validation Standard VS-2 Computer-Related System Validation. Barbara Mullendore, Kenneth G. Chapman. Journal of Validation Technology. Volume 7, Number 3. May 2001.
- 12 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.
- 13 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.
- 14 Medical Device Quality Systems Manual - 4. Process Validation. U.S. Food and Drug Administration - Center for Devices and Radiological Health. <http://www.fda.gov/cdrh/qsr/04valid.html>. January 1997.
- 15 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.
- 16 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.
- 17 GLP Consensus Document the Application of the Principles of GLP to Computerised Systems, Environment Monograph N^o. 116. - OECD Series on Principles of Good Laboratory Practice and Compliance Monitoring - N^o 10. Organisation for Economic Co-Operation and Development. [http://www.oecd.org/olis/1995doc.nsf/LinkTo/NT00000C06/\\$FILE/ENE51434.PDF](http://www.oecd.org/olis/1995doc.nsf/LinkTo/NT00000C06/$FILE/ENE51434.PDF). 1995.
- 18 PIC/S GMP Guide to Good Manufacturing Practice for Medicinal Products Part II. PIC/S - Pharmaceutical Inspection Convention and Pharmaceutical Inspection Co-Operation Scheme. http://www.picscheme.org/publis/guides/PE_009-8_GMP_Guide%20Part%20II_Basic_Requirements_for_API.pdf. January 2009.
- 19 ISO/IEC 14598-4:1999 Information technology. Software production evaluation. Process for acquirers. International Organization for Standardization. 1999.
- 20 GAMP® Good Practice Guide: Calibration Management. ISPE. Dec 2001.
- 21 Good Practice and Compliance for Electronic Records and Signatures Part 1 - Good Electronic Records Management (GERM). ISPE, PDA. 2002.
- 22 Good Practice and Compliance for Electronic Records and Signatures Part 2 - Complying with 21 CFR Part 11 Electronic Records and Electronic Signatures. ISPE, PDA. 2001.
- 23 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/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm089543.htm>. May 2005.
- 24 Glossary of Computerized System and Software Development Terminology. Inspection references: Inspection Guides. U.S. Food and Drug Administration Office of Regulatory Affairs. <http://www.fda.gov/ICECI/Inspections/InspectionGuides/ucm074875.htm>. August 1995.
- 25 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.
- 26 Validation in Blood Establishments and Transfusion Services. AABB Press. 1996.
- 27 ISO 9001:2008 Quality management systems. Requirements. International Organization for Standardization. November 2008.
- 28 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. <http://www.fda.gov/cdrh/comp/guidance/1553.html>. January 2005
- 29 GAMP® Good Practice Guide: Electronic Data Archiving. ISPE. July 2007
- 30 GAMP® Good Practice Guide: Testing of GxP Systems. ISPE. Dec 2005
- 31 GAMP® Good Practice Guide: IT Infrastructure Control and Compliance. ISPE. Sept 2005
- 32 GAMP® Good Practice Guide: Validation of Laboratory Computerized Systems. ISPE. April 2005. ISBN 1-931879-39-7.
- 33 GAMP® Good Practice Guide: Risk-Based Approach to Electronic Records and Signatures. ISPE. Feb 2005
- 34 Guide to the Preparation, Use and Quality Assurance of Blood Components 14th Edition. CoE. 2008.

12. Acronyms

- DS: Design Specification
 FS: Functional Specification

GAMP®: Good Automated Manufacturing Practice

GCP: Good Clinical Practice

GLP: Good Laboratory Practice

GMP: Good Manufacturing Practice

GxP: Good 'x' Practice, where 'x' represents:

- Clinical
- Quality
- 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

13. 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.

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 programs, 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 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.

Computerised 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 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 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.

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 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 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 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 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 are 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	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 User
Risk assessment	Risk analysis	User
Validation plan	Validation plan Validation protocol	User 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
Business continuity plan	Countermeasures plans Disaster recovery plans Continuity action plans	User and Supplier
Problem resolution	Problem resolution records	User
Validation report	Validation report	User
In operation	Maintenance, calibration and monitoring plans and records Periodic audit /review plans and reports Change control and incident records Data migration plan Change notification	User Supplier
System retirement	System retirement plan and report	User

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

SOPs	Supplied by
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® 5 A Risk-based Approach to Compliant GxP Computerised systems [1] and the PIC/S Good Practices for computerised Systems in regulated 'GxP' environments [4] 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).

Category 2: No longer used

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: Non-configured products

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 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 organisations 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 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 organisations 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).

Examples of classifications 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 pressure automated system	1
Blood product storage devices	4
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

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