APPENDIX I

Planning and Implementing System Change

This section covers the initial steps for implementing a new system into the transfusion department. Many of these steps will also apply to major upgrades and to separate procurement of subsidiary systems such as analytical systems and associated middleware and electronic blood administration (tracking) systems.

A.1 Business Case

The business case captures the reasons for initiating the purchase of a new or updated system and identifies resources, either capital, revenue or staff, that will be required to deliver the specific business need. Information in a formal business case should include the background of the project, the expected business benefits, the options considered (with reasons for rejecting or carrying forward each option), the expected costs of the project, and the identified risks. IT systems may qualify as an in vitro diagnostic (IVD) medical device as set out in Directive 98/79/EC and as such these regulations must be taken into account [1].

The business case will need to be developed in line with local policies, but the output should clearly identify:

- The scope of the project – what is included and what is excluded with clear boundaries;
- Management responsibilities, identifying the project owner and project team members;
- Resources required for the project (staff, equipment, accommodation and financial).

The business case must also consider the impact on linking to other systems, both within the organisation (e.g., Patient Administration Systems [PAS], Electronic Patient Records [EPR]) and outside [e.g., links with Primary Care & Blood Establishments]), and Electronic requesting systems and define how this will be managed and the degree of interaction permitted between the systems.

A.2 Project Planning

Once the business case has been approved the project planning approach needs to be defined. A multi-disciplinary team, including subject matter experts, IT personnel and a project manager should be established and a project plan and project quality plan created. This will help to ensure the necessary controls are in place and managed under the regulatory framework. The transfusion requirements for an IT system may be very different from broader Pathology requirements. Potential systems must be fully evaluated to ensure compliance with the transfusion requirements.

Where a new system will bring together information from multiple existing PAS or Laboratory Information Management Systems (LIMS), particular care needs to be taken to ensure that differences in the way information has been structured and entered in these systems is taken into account (e.g., code tables, locally agreed terms and abbreviations etc.). Assumptions about the compatibility of information cannot be made and each system should be fully assessed in its own right at the outset.

Project Management must include:

- **Change Management -** A new LIMS or an upgrade to the current LIMS must be managed under the formal change control system in operation within the organisation.

- **Risk/impact assessment -** In any project a risk assessment must be performed to identify all the factors that impact on the project itself or continuing service provision and define ways to mitigate the identified risks. Risk assessment must be ongoing throughout the project and should be used to focus the validation effort on the higher risk areas.
- **Responsibilities and authorities -** The project management documentation should include: project scope and boundaries; project management and delivery approach; roles and responsibilities; project governance; resource management; quality assurance.

A.3 Process Maps

It is important to gain a common understanding of the entire process, the specific roles and contributions of personnel, process inputs and outputs and the interactions of the LIMS system with external IT systems/devices. This can be achieved using a process mapping technique. All processes within the scope of the project should be mapped, together with relevant boundary processes.

Implementation of a new system may impact and change existing processes. Where this occurs, both existing and new process flows should be mapped to help understand the impact of the changes[2].

This type of mapping will help to formulate the detail of the User Requirement Specification (URS). It is also a valuable tool in system configuration to ensure that all necessary process interactions are supported.

A.4 User Requirement Specification

System requirement specifications are created at a number of levels of detail and points in a system lifecycle. The initial specification often called the Operational Requirement Document (ORD) is created during the system procurement process. It is used to inform potential

suppliers of what process or processes the system is expected to support and the functionality it is expected to provide. Depending on the complexity of the process the requirements in the ORD may be broken down into more detailed requirement specifications often referred to as the URS. Following initial implementation as time progresses business requirements often change and this will require amendments to system configuration and in some cases additional functional development. For each change required a further specific URS should be created specifying the amendments now required. An example of the basic information required in the ORD and URS is shown in Appendix IV.

The Operational Requirement Document

The ORD is a structured document which identifies all of the essential and desirable requirements of the system and will be issued to potential suppliers with the invitation to tender. Each requirement should be clearly marked as essential or desirable, recognizing that failure to satisfy all essential requirements will eliminate a bid. This is the document which informs suppliers what a system is required to do. This document should be at a relatively high level with the requirement statements saying in broad terms what functionality is required e.g., "the system must allow for the registration of the mandatory patient demographics; mandatory identifiers are…". At this stage it is an open statement and suppliers will be asked to demonstrate that as minimum the mandatory identifiers can be registered. During the procurement process suppliers who can meet this requirement will pass on this point however some suppliers may be able to demonstrate that they can accommodate not only the mandatory identifiers but a whole host of other useful patient data and therefore on this point may become the preferred option. The ORD should be used to draw out information about the system capabilities, ensuring that all mandatory

requirements will be met. It is a contractual document which a supplier can be held to deliver however the onus will be on the organisation to prove non-compliance with a requirement.

For complex sets of requirements or where requirements must be delivered in a more precise manner it may be necessary to give a more detailed insight into a requirement. In this case a detailed User Requirement Document (URS) may also be created however the same fundamental principles apply for both documents and the terms ORD and URS are often used interchangeably. URS is the more common term and will be used for the rest of this document.

The User Requirement Specification

In developing the URS, consideration should be given to current and future developments in the field of transfusion medicine information management. The document should be developed by a multi specialist team and should include specialist subject matter experts from the laboratory, clinical teams including consultant involvement and Trust and Laboratory IT.

As modern LIMS offer extensive configurability it is important to specify in the URS what is required, but to avoid specifying how it is to be achieved unless this is essential to the operational need.

A.4.1 Operational Functionality

The URS is a structured document. Every functional requirement of the system needs to be detailed within the URS. Requirements should be written in clear numbered paragraphs, with each paragraph identifying a single requirement. Each requirement should be written so that it clearly specifies what is required giving any specific capabilities and the criteria against which compliance will be measured. This format ensures clarity and provides a means to

reference validation evidence back to requirements. Vague and ambiguous statements must be avoided.

The writing group have provided a sample URS/ORD as part of the guideline to provide assistance in writing such documents. This contains a small number of examples and is not intended to be a complete example.

A.4.2 Validation Requirements

The URS should outline the validation/qualification strategy and clearly define the roles and responsibilities of both the supplier and purchaser. For this reason, it is important to specify requirements such that they can be readily tested and evidence provided of both compliance and non-compliance with the requirement statement. In a procurement situation validation will be at two levels. Level one is to validate that the supplier is offering a system that has the potential to fulfil the operational requirements. Level two is to validate that on implementation the system actually does sufficiently meet the requirements in a way that is operationally fit for purpose.

A.4.3 Interface Specification

Many instruments and analytical devices provide a means of communicating electronically with LIMS however there is a lack of standardisation in this area and communication formats vary from device to device. An example of a commonly occurring interface is that between a grouping analyser and the LIMS. Interface software provides a mechanism to convert the communication from the instrument to a format the receiving system can understand.

Some specialist interface software, known as middleware, may be used to allow multiple analysers and multiple sites to communicate with the LIMS using a common format. Middleware may also undertake some interpretation of raw data to provide a test conclusion

to the LIMS. A decision needs to be made and recorded as to whether or not the interpretation of results is undertaken by the LIMS or by the middleware. Any system undertaking interpretation of results is classified as a IVD medical device and as such is must meet the specifications set out in Directive 98/79/EC[1].

All required interfaces (current and anticipated) should be identified in the URS. Details should include: the data which is to be transferred; batch or real time transfer, error detection and alarms. Equipment suppliers can usually provide communication specifications for the interfaces to connect their equipment to LIMS which will also indicate what data and/or flags can be transmitted.

When specifying interface requirements consideration should also be given to ensuring support of existing and developing information transfer standards to increase flexibility and reduce the overhead of future change.

A.4.4 Electronic Data Interchange (Interoperability)

System to system communication is an essential requirement of healthcare computing. The LIMS will need to be able to communicate with other systems including the PAS, Electronic Request Systems (Order Comms) and Electronic Blood Management/Tracking systems. There is a growing expectation for seamless information sharing between systems and this needs to be supported by effective interoperability.

Electronic Data Interchange (EDI) is the term used to describe the structured messages and protocols used for such communications in a way that the receiving system can correctly interpret the value, meaning and context of the information sent from the transmitting system. Required EDI functionality should be identified, and EDI standards that are used within the national and local healthcare IT environment should be specified.

Interfaces between computer systems, in particular between the PAS and LIMS must be configured and validated to ensure compatibility between the information formats used by each system. Care should be taken to ensure no pre-existing LIMS data is altered automatically by PAS links. Any such alterations would be by positive authorised user action within the laboratory.

EDI may be unidirectional such as the Electronic Delivery Note (EDN)[3] used to send information from blood services to hospitals using a fixed format file, or may be bi-directional such as the information interchange that occurs between an electronic request system (Order Comms) and a LIMS during ordering of blood components. There is an expectation for seamless information sharing between systems and this needs to be supported by effective interoperability. An example of interoperability is shown in Figure 1.

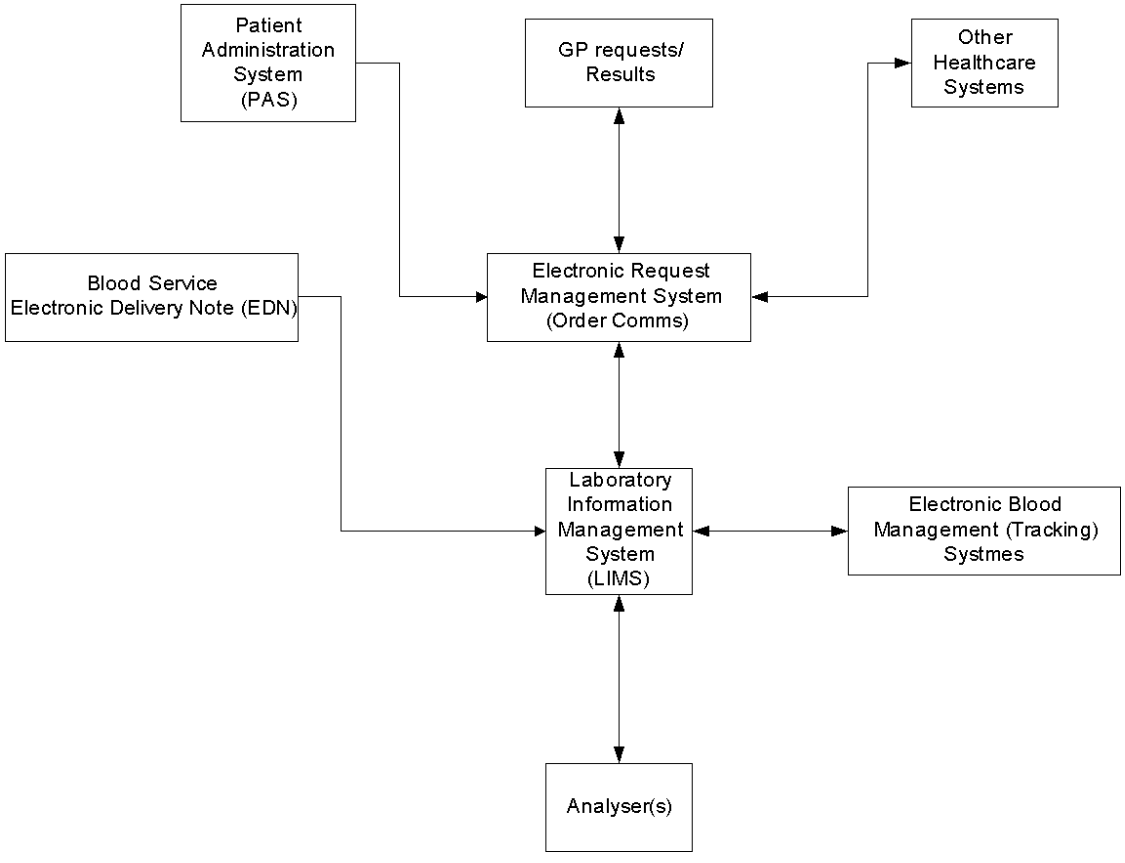

Figure 1: An example of interoperability.

Abbreviations: EDN: Electronic Delivery Note; GP, general practitioner; PAS, Patient Administration Systems; LIMS, Laboratory Information Management Systems

A.4.5 Peripherals and Hardware Requirements

Any items of hardware should be appropriate in terms of specification and numbers to ensure the running, security and performance of the software application. To ensure that the necessary requirements are met the following should be considered when purchasing:

- Number of concurrent users
- Maximum transaction rate to be supported
- Anticipated growth rate
- Resilience to single point of failure

A.4.6 Operational Environments

An operational environment is a version of the system (software, hardware, peripherals) used for a specified purpose. The 'live' environment is the one in routine use on a day to day basis. All systems should support multiple environments with a minimum of two environments to allow a separation of live and validation/training environments. The optimum set up would include environments for test, validation, live, training and disaster recovery (DR) although it's recognised that DR may need to be on a separate server/installation. Each environment must be completely independent and version controlled. Modern configurable systems may support larger numbers of environments and users should specify the number and type required in the URS.

All environments will need to be able to link to other operational systems (e.g., Order Comms). Consideration must be given to how this can be achieved without impacting on live data and live operational use.

A.4.7 Data Management

The information held on existing systems forms an essential record, some of which falls within the record retention requirements of the Blood Safety and Quality Regulations (BSQR) and the Medicines and Healthcare products Regulatory Agency (MHRA) 'GXP' Data Integrity Guidance and Definitions [4]. In addition, much of this information is critical to the ongoing operation of the department. It is therefore of critical importance to ensure that the management of this information through the system transfer and into the future is well defined and captured within the URS. This is an area where typically the ORD states if migration of legacy data into the new system is required and if it is a more detailed URS is created to specify the exact data to be migrated. Data that needs to be retained may either be migrated to the new system or may be archived in a manner that makes it accessible for lookback purposes.

The decision on whether this data is migrated or archived will depend on several factors. These will include: the historic data needs of the new system; the proposed manner in which the new system interacts and displays historic data; the quality of the legacy data; and the cost effectiveness of archiving versus live database retention[5]. It is recommended that a formal risk assessment is performed to determine the most appropriate approach.

A.4.7.1 Data Migration

Data migration is the process of moving stored data from one durable storage location to another. This may include changing the format of data to make it more usable or visible on an alternative computerised system, but not changing the content or meaning. Data transfer/migration procedures should include a rationale and be robustly designed and validated to ensure that data integrity is maintained during the data lifecycle [4]. Careful

consideration should be given to understanding the data format and the potential for alteration at each stage of data generation, transfer and subsequent storage and should take into account:

- Legal requirements (e.g., traceability as defined by the BSQR [5] in terms of the final fate of all components).
- Operational requirements (e.g., historic group, antibody information, special requirements).

The most direct form of migration is to transfer records directly into the new database although data reformatting may be required. Where any form of data migration is performed it is important that the quality of data migrated is verified (see section A.7.1). All patients must be uniquely identified and should have an NHS number (or equivalent)[6].

In more complex situations where information from multiple legacy systems is being transferred into a single new system, variations in the use of key identifiers and the format of data can cause difficulties.

Secure operational procedures must be in place to ensure data integrity and minimise the potential for incorrect linking to occur. Each piece of data may need to be evaluated through a number of phases before migration to the new system. A full audit trail for this process is essential.

Retaining operational data on a legacy system that is not electronically linked to the operational system (i.e., interrogating a separate database which is a manual step), is not acceptable for maintaining patient safety within the transfusion laboratory.

A.4.7.2 Archive Data Storage

Some data may not be required for routine operational purposes but will need to be retained for “lookback”/audit. Where it is decided not to migrate this data consideration will need to be given to ensuring that it remains readily accessible. It is important that the archived data can be searched using search criteria including: patient identifiers; donation number; and batch/lot number to ensure all “look back” requests can be met. It is essential to ensure the same data security controls are applied to the archived data as apply to the live system.

There are several possible archiving options including:

- Migrate the data into a data warehouse or equivalent reference database;
- Maintain the legacy system in a non-operational, read only configuration (see below).

Managing legacy systems may be complex and costly. Consideration must be given to the long term sustainability. (The current regulation for data retention, at present, is a minimum of 30 years)[5].

In order to effectively maintain the legacy system the following requirements will need to be met:

- Adequate backup of the legacy database.
- Ongoing system maintenance contract and licensing.
- Regular start up and running of system.
- Maintaining staff access to and skills in the use of the system.
- Regular “lookback” validation exercises.
- Regular review to ensure ongoing hardware and software support.
- Planning for ongoing migration or archiving when system can no longer be supported.

Regular Audit of who is accessing the system is required to ensure there are personnel who remain competent at accessing the legacy system. The archiving strategy documentation needs to be retained to support "lookback" activity. Whichever approach is adopted the archive system must be fully supported with Standard Operating Procedures (SOPs) and staff training. Included in this documentation will be the requirement to develop new SOPs to ensure "lookback" activity is controlled.

It may be appropriate to categorise the legacy data into that which will be migrated to the new system and that which will be archived. This may be done on the basis of time (e.g., data from the last five years is migrated and prior data archived) or maybe specific to information types depending on the database structure (e.g., it may be more important to transfer patient information, blood group and antibody status than test data and component details). Where an existing database is to be split into data for migration and data for archive careful consideration needs to be given to the boundary cases to ensure there is a clean division.

Consideration should also be given to how data is matched/linked when storing data from more than one site. This is especially important where the format of data held on each site prevents an exact match.

A.4.8 Maintenance Requirements

The maintenance of the system will include aspects which are undertaken by the Trust/Hospital IM&T department as well as those which are in the remit of the supplier. Responsibilities must be agreed and covered by relevant contractual agreements.

A.5 Procurement

Procurement of a LIMS will require a multi-disciplinary approach and will need to follow the healthcare organisations purchasing procedures. Requirements should be clearly identified as “essential” or “desirable”, recognising that a bid that fails to provide all “essential” requirements would be eliminated from consideration. Any weighting to be applied to the bid evaluation should be pre-determined and documented prior to the release of the tender invitation.

A.5.1 Bid Evaluation

Bid evaluation will follow standard procurement procedures for the specific organisation and will include financial considerations. A technical evaluation using a scoring and weighting system should be employed in order to compare the degree of compliance of submitted bids to the URS. Bids will only be technically acceptable if all essential requirements have been addressed. Some bidders may indicate that essential requirements are not currently supported and can be developed and the evaluation scoring system will need to consider how to address this.

A.5.2 Gap Analysis

Once a supplier has been selected, the process maps, URS and technical evaluation should be used to identify all areas of the selected system where there are identified gaps, for e.g. desirable requirements that are not met.

These gaps may be addressed by:

- Modification of the new system either prior to installation or as an upgrade following installation.

- Modification of existing operational processes to address the gap outside of the new system.
- No action required, limitation accepted.

In all cases a risk assessment should be performed to determine the appropriate action and decisions documented. Where change is required this should be handled through a formal change request process with the supplier.

A.6 Contract

Once the tendering process is complete and a supplier has been selected there will be a phase of contract negotiations to ensure all parties are clear on their responsibilities and commitments. Negotiations may include:

- Project management responsibilities of supplier and purchaser.
- Communications between parties.
- Identification of any changes required as a result of the gap analysis of the bid.
- How training is to be delivered.
- Documentation and technical support arrangements.
- Implementation planning and support.
- Configuration support.
- Testing and validation support.

Good Automated Manufacturing Practice 5 (GAMP5)[6] category classification provides guidance on what the Supplier should deliver for the lifecycle of the system.

A.7 Implementation Preparation

This section addresses tasks which will need to be completed prior to implementation, some of which may be undertaken concurrently with earlier stages of the procurement process.

A.7.1 Data Cleansing

Data in an established database is rarely 100% consistent and accurate. Anomalies and corruptions of data can occur for a variety of reasons and whilst these may not cause problems in their home system, problems can arise when the data is migrated. Data cleansing is a structured approach to examining and analysing an existing database with a view to identifying and correcting anomalies prior to migration. This is an essential process, particularly when migrating data across organisations or across networks and a strategy and methodology should be defined to ensure that it is effectively managed. Data cleansing should be carried out in a quality controlled manner with fully documented procedures in place. Critical areas include patients with antibodies (ensure all codes match across data to be migrated) and patients with special requirements.

A.7.2 Duplicate Records

Searches for duplicate records should be regularly carried out on the legacy system and duplicates resolved prior to data migration.

A.7.3 Implementation Strategy

An implementation strategy is required to define how the new system will be brought into routine operation. The implementation of a new LIMS must be managed in a manner that will meet the regulatory requirements. The strategy to be adopted will depend on several factors including:

- The degree and complexity of data migration.
- Whether multiple legacy systems are being combined.
- Staff resources, space and infrastructure availability.
- Available operational environments.

Consideration must be given to the impact of the implementation on the routine operation of the laboratory. There will necessarily be operational downtime associated with data migration, system configuration and physical connectivity. This will necessitate the transfusion laboratory implementing business continuity plans and engagement with clinical and administrative services to manage interruptions of service and the recovery phase.

Whichever implementation strategy is decided upon appropriate risk management plans must be developed. Possible strategies include:

A.7.3.1 Parallel Running

In parallel running both new and old systems are run together with the routine workload being put through both systems. This involves migrating data from the old to the new system, performing each action in the appropriate areas on both systems. Parallel running allows staff to become fully familiar with full load running of the new system prior to 'go live' and can provide a high level of assurance that the new system is performing as expected post implementation. However such an approach will be resource hungry in terms of staff input. A variation to this approach may involve running only a proportion of the workload in parallel.

The parallel running approach may be facilitated or limited by instrument interfaces, blood management systems, power and IT points availability. It is not always possible to send instrument data to two interfaces or systems simultaneously. Switching an instrument interface between two LIMS systems or environments needs careful control to ensure no

changes are made that will require validation. The functionality of the instrument interfaces needs to be understood and carefully managed.

A.7.3.2 Phased Approach

This will involve staff using both systems whilst transferring specific functions or sites from the existing to the new system over a period of time. The decision will involve identifying when operational areas are to be transferred. This method presents some technical and logistical difficulties such as data transfer and managing the boundaries between functions running on each system. Each step of a phased approach will need its own risk assessment to address these challenges.

A.7.3.3 Big Bang

This approach will ensure total transfer to the new system on a defined date. The organisation must ensure that procedures have been written and validated, staff have undergone thorough training, in every area, prior to "go live" and that trial transfer has been run on test environments. The implementation plan should include a "fall back" plan in the event of a major problem preventing completion of the implementation within the determined time frame and should identify the "point of no return" where outstanding issues must be resolved without fall back.

A.7.4 Validation Strategy

The validation strategy should comply with regulatory requirements and associated guidance, taking into account the principles of GAMP5[6] as set out in the BSH Guidelines for Validation & Qualification including Change Control, for Hospital Transfusion Laboratories[7] and the

International Society of Blood Transfusion (ISBT) Guidelines for the Validation of Automated Systems in Blood Establishments[8].

A.7.5 Application Configuration

LIMS solutions take advantage of techniques in software design that are inherently configurable and adaptable. In order to configure such systems to operate to the requirements of a particular organisation a set of logic rules and configuration settings has to be established and applied.

These logic rules and configuration settings ensure that, under a defined set of circumstances, the system will consistently take the actions specified. This is a powerful tool to ensure reproducibility of actions and it is essential that they are established, managed and monitored closely. Staff who are designated to configure the system, often referred to as “super-users”, should be trained and competent prior to beginning the configuration of the system. The involvement of an individual who is a transfusion expert is imperative. They should have overall responsibility for determining what the rules and settings should be and the appropriate validation steps in agreement with the Hospital Transfusion team, in order to ensure results and actions support good transfusion practice. This individual may be supported by other super-users.

The computer follows the rules specified and is a valuable asset in terms of security. Care must be taken to set up and test rules to ensure they are comprehensive and patient safety is not endangered through an incomplete rule set. The risks/benefits should be assessed before each rule is implemented. Rules may require an “over-ride” function to deal with legitimate exceptions. If incorporated, this must be available only at defined security levels and if used the system should require and document a reason.

Examples of scenarios that may be controlled through configuration include:

- Associating user and supervisor alert flags with a specific result profile.
- Enabling the issuing of blood & components by authorised staff
- Prompting users to perform specific follow up actions or reflex testing (e.g., request additional samples, issue a specific blood product).
- Setting action reminders or flags into the patient record.
- Determining whether a patient is suitable for electronic issue of blood.
- Helping to prevent issue of incompatible units (e.g., patients with antibodies).
- Helping to ensure appropriate blood products are issued to a patient (e.g., depending upon their gender/age details prompting selection of appropriate units such as K-, CMV negative etc.).
- Ensuring appropriate comments are added to reports.

A selection of logic rules, based on BSH guidelines and good practice is supplied in Appendix II.

A.7.6 Data Migration Preparation

Achieving an accurate data migration will be an iterative process which may be time consuming and will require close co-operation between laboratory staff, IT specialists and the suppliers of both the legacy and the new system.

The iterative loop has several distinct steps which include:

- Identify the data to be migrated giving clear, documented rationale for the decisions made.
- Document the structure and meanings of all fields and values to be migrated and build necessary translation tables[9].

- Extract the required data into a separate file/table/database.
- Transformation: manipulate and format the extracted data for upload to the new system ensuring the transformations accurately map data content and meaning.
- Upload data into new system.
- Create an audit log detailing all steps in the process (who, what, when and why).
- Define the number of records for verification, and the process for selecting a representative sample.
- Perform data verification.
- Identify migration failures and assess impact.
- Revise migration tools as required.

Validation of data migration is a critical process and requires careful planning. The scope of the validation will need to include external systems that interact with the LIMS data. Defining the sampling plans of migrated data can be undertaken using a risk based approach.

A.7.7 Training Strategy and Plan

The training requirements for implementing a new LIMS should not be underestimated and it is important that a critical mass of staff is fully trained prior to implementation. The contract with the supplier should identify where the responsibility for training lies and how this will be delivered (e.g., direct training, train the trainer). The training requirements within the organisation should be evaluated to identify:

- Who to train - e.g., Blood Sciences/IT/Clinical staff.
- What to include - e.g., Discrete areas/whole system.

Before training can commence SOPs/training manuals should be completed, as a minimum in draft format.

All staff involved in the development, running and maintaining of the LIMS will require training and competence assessment which is relevant to the role and these will determine the level of security access permitted. Assessments should be completed and signed off prior to granting access to the live system.

The training and competency assessment programme should be reviewed on a regular basis and following any software upgrades.

A.8 Service Level Agreements

In addition to maintenance contracts held directly with system suppliers, there must be a specific Service Level Agreement (SLA) between the transfusion department and any other IT service provider (internal or external) whose activities could impact the LIMS or associated systems. Such SLAs must clearly define the service provision, controls and authorisations, and performance expectations for any IT support arrangements including system data backups.

A.9 User Configuration Verification

Prior to validation the users should perform informal testing to ensure the system has been configured appropriately to support operational requirements. This is an informal testing process that:

- Familiarises staff with the system.
- Allows the development of SOPs which are required for validation.
- Ensures that the system configuration meets the users' needs.
- Reduces the time required for formal validation.

Any configuration changes identified should be implemented prior to formal validation. The system must be placed under change control on commencement of formal validation to ensure that any future changes are appropriately controlled.

A.10 Validation

The Validation strategy will have been determined during implementation preparation (see section A.7). Validation is the formal testing and ensures that the system meets the operational requirements of the URS. Both supplier and user will have responsibilities for validation and these should be in line with the BSH Validation and Qualification guidelines[7].

The content and scope of validation is well documented in the ISBT Guidelines for the Validation of Automated Systems in Blood Establishments[8] which has application for hospital transfusion laboratories and the Guidelines for Validation and Qualification, including Change Control, for Hospital Transfusion Laboratories[7].

Recommendation:

- **A formal process of change control is essential when implementing a new IT system. All of the steps identified in section I are necessary and must be adequately resourced and change controlled (2B).**

1. Medicines and Healthcare Products Regulatory Agency. *Guidance on the regulation of In Vitro Diagnostic medical devices in Great Britain.* . 2023 [cited 2023 19/06/23]; Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/946260/IVDD_legislation_guidance_-_PDF.pdf.
2. NHS Digital. *Data Security and Protection Toolkit*. 2022 [cited 2023 20/06/23]; Available from: https://digital.nhs.uk/data-and-information/looking-after-information/data-security-and-information-governance/data-security-and-protection-toolkit.
3. Sampson, J., et al., *ISBT Guidelines for Validation of Automated Systems in Blood Establishments.* Vox Sanguinis, 2010. **98**(suppl 1): p. 1-19.
4. Medicines and Healthcare Products Regulatory Agency (MHRA). *GXP Data Integrity Guidance and Definitions*. 2018 [cited 2023 20/06/23]; Available from: https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/687246/MHRA_GxP_data_integrity_guide_March_edited_Final.pdf.
5. UK Government. *The Blood Safety and Quality Regulations 2005 (as amended) SI 2005/50*. 2005 [cited 2023 19/06/23]; Available from: https://www.legislation.gov.uk/uksi/2005/50/contents/made.
6. Andrews, S., *GAMP® 5: A Risk-Based Approach to Compliant GxP Computerized Systems*. 2nd ed. 2022, International Society for Pharmaceutical Engineering, Tampa, Florida.

7. Nightingale, M., *Validating data migrated onto information technology (IT) systems.* Pharmaceutical Engineering, 2011. **31**.
8. NHS Digital. *https://www.gov.uk/government/publications/in-vitro-diagnostic-medical-devices-guidance-on-legislation*. 2023 [cited 2023 13/07/2023]; Available from: https://digital.nhs.uk/data-and-information/information-standards/information-standards-and-data-collections-including-extractions/publications-and-notifications/standards-and-collections/isb-0149-nhs-number.
9. The Royal College of Pathologists. *The retention and storage of pathological records and specimens (5th edition)*. 2015 [cited 2023 19/06/23]; Available from: https://www.rcpath.org/static/049ea966-df5c-4a9f-9353ba24a69bb808/The-retention-and-storage-of-pathological-records-and-specimens-5th-edition.pdf.