Validation Approach

Project management plan

All Thermo Fisher Scientific implementation projects produce a Project Management Plan (PMP) to specify scope, applicability, and quality criteria for individual projects. The PMP is stored during the project in the Thermo Fisher filing system.

Early in the project, our Thermo Fisher brands Project Manager will produce the PMP and it is required that the PMP be signed and approved by the Project Manager from both parties, Customer and Service Provider. Once the PMP has been signed and approved, it should not be changed without formal Change Control Management.

The PMP is under the responsibility of the Service Provider.

System validation plan

The System Validation Plan describes the detailed system scope, validation methodologies, validation activities and validation deliverables of the validation project.

The Validation Plan must be signed and approved by both parties, Customer and Service Provider. Following signature and approval, the Validation Plan will be maintained through Change Control Management.

The Validation Plan is typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

Requirements management

Requirement management is an essential part of an efficient validation process. Requirements are expected to change and evolve during the project. The requirement's list is part of the Project Backlog and is maintained through Change Control Management. The requirements list will be gathered by Service Provider and put into a Requirements Trace Matrix (RTM). Following, the RTM will be uploaded into JIRA to fill the Project Backlog (**https://thermofisher.atlassian.net**).

Each Backlog item will be evaluated to be identified as either Standard, data setup, configuration (Out of the Box functionalities) or Development (C#, VGL).

The Requirements Management is under the responsibility of both sides, the Service Provider and the Customer.

GxP criticality assessment and risk assessment (risk-based approach or not)

All functions could affect the integrity or availability of the analytical record. Therefore, all functions are critical and will be addressed by the validation. A detailed breakdown of the risk analysis by requirement is not necessary, as most functions are critical. Risks that are identified during the Requirements Management process are considered Project level risks.

In the context of a Risk-Based Validation approach, we can assume that standard functionalities are already validated according to the software validation guidelines. The evidence can be brought by organizing an Audit in our Manchester office in the United Kingdom.

In addition to this risk assessment, testing incident (deviation) resolution will include a risk assessment. Each individual incident will be assessed for risks associated and their impact, likelihood, and likelihood of detection. This risk assessment will then be used to determine incident resolution.

Risk management will be ongoing throughout the project. For example, as stated in the PMP, re-appraisal of risks will be a part of the procedure for producing monthly project update reports. All validation summary reports will include risk assessment.

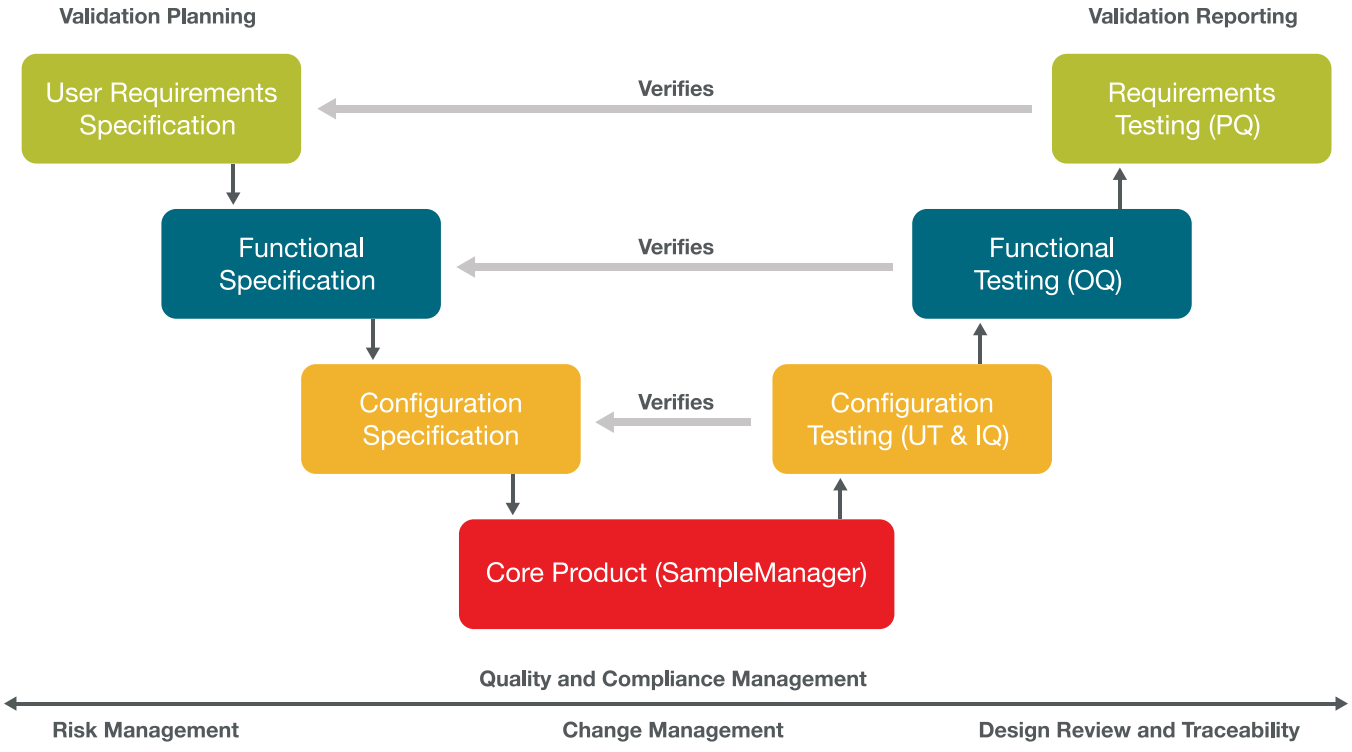
The Risk Assessment is typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

Traceability matrix

The Traceability Matrix is made to link the User Requirements Specifications (JIRA backlog Items) to the Functional and Design Specifications and Test Scripts as defined in the V-model diagram above.

For standard functions, our Thermo Fisher Traceability Matrix already exists which refers to Standard functionalities, Specifications and Unit Tests. This Matrix is included into the Standard Validation Kit (additional cost). An audit in our UK office can also be arranged to verify the conformity of our Core Product according to the Validation guidelines and then only focus on Configurated / Developed functionalities in the Validation efforts (Risk-Based Validation approach).

The Traceability Matrix is typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.



Change control
In accordance with GAMP guidance, Change Control procedures will be executed and documented within JIRA (**https://thermofisher.atlassian.net**). All deliverable working items will be kept and tracked with a version.

The Change Control System is typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

Standard operating procedure
In order to facilitate efficient and controlled system operations, several Standard Operating Procedures (SOPs) are required. SOPs are needed to cover usage and maintenance of the system. SOPs are related to on-going system procedures and maintenance.

SOPs will be assessed by the Customer in consultation with the Service Provider.

The SOPs are typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

Functional requirements specs and design specs
It is a specific requirement of GAMP and of various regulatory bodies that functional and design specifications are produced for computer systems used in a regulatory environment. The functional specification should specify the product in terms of the functions it performs to meet User Requirements. The functional specifications will be the main input of the OQ script writing process.

It is essential that both Service Provider and Customer approve the functional specifications before the Execution Step.

On a “risk-based” Validation approach, the only items validated are the configured / customized functionalities requested by Customer in accordance with Contract terms and Conditions, as it is assumed that the Standard Functionalities are already validated.

The Design Specifications are typically under the responsibility of both sides, the Service Provider and the Customer.

Important note: The standard must be prior to the configured / developed functionalities to limit the impacts on the cost and Schedule Baseline. The quality grade of the design specifications will be evaluated according to the Cost and Scheduled constraints.

Security specifications & policy
The security specification will address both physical and logical security controls to be applied to the application, and operating system, storage media, equipment, and documentation. An access control matrix will define the various classes of users, the various classes of data/ information, and the access privileges (e.g., create, read, update, delete) for each combination of user and data. Application-level privileges will be specified with existing business area practices and procedures.

The Security Specifications are related to the overall environments, Operating System, Network and Software.

The Security Specifications & Policy are usually typically the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

Tests strategy

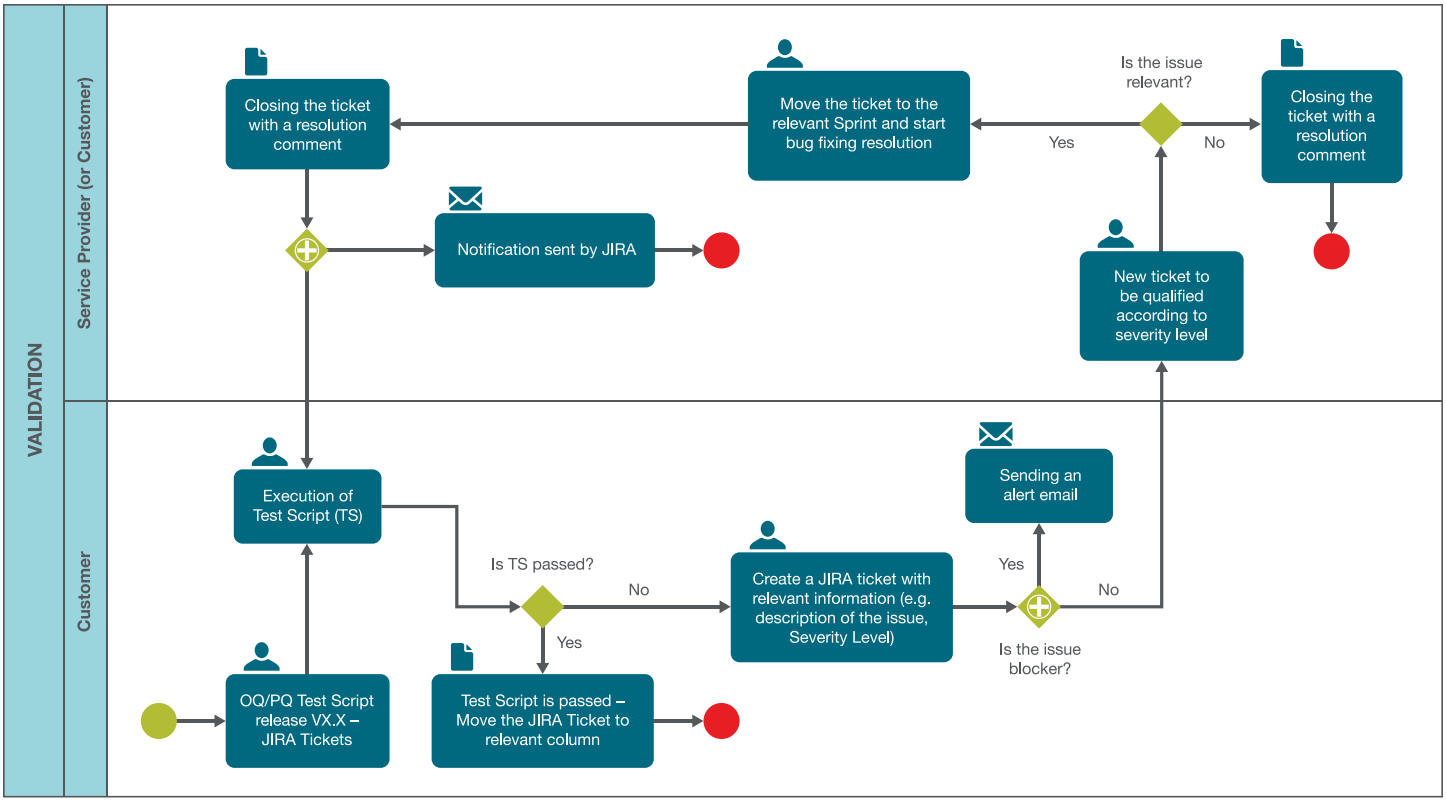
The Test Strategy defines the procedure for all software testing, including installation testing (IQ), system and integration testing (OQ), and user acceptance testing (PQ).

Items defined in the Test Strategy include, but are not limited to, the following:

- Procedure for recording test evidence (screenshots, signatures etc)
- Procedure for pre and post-test approval of scripts and protocols
- Procedure for recording and resolving failures and incidents, including any necessary retesting

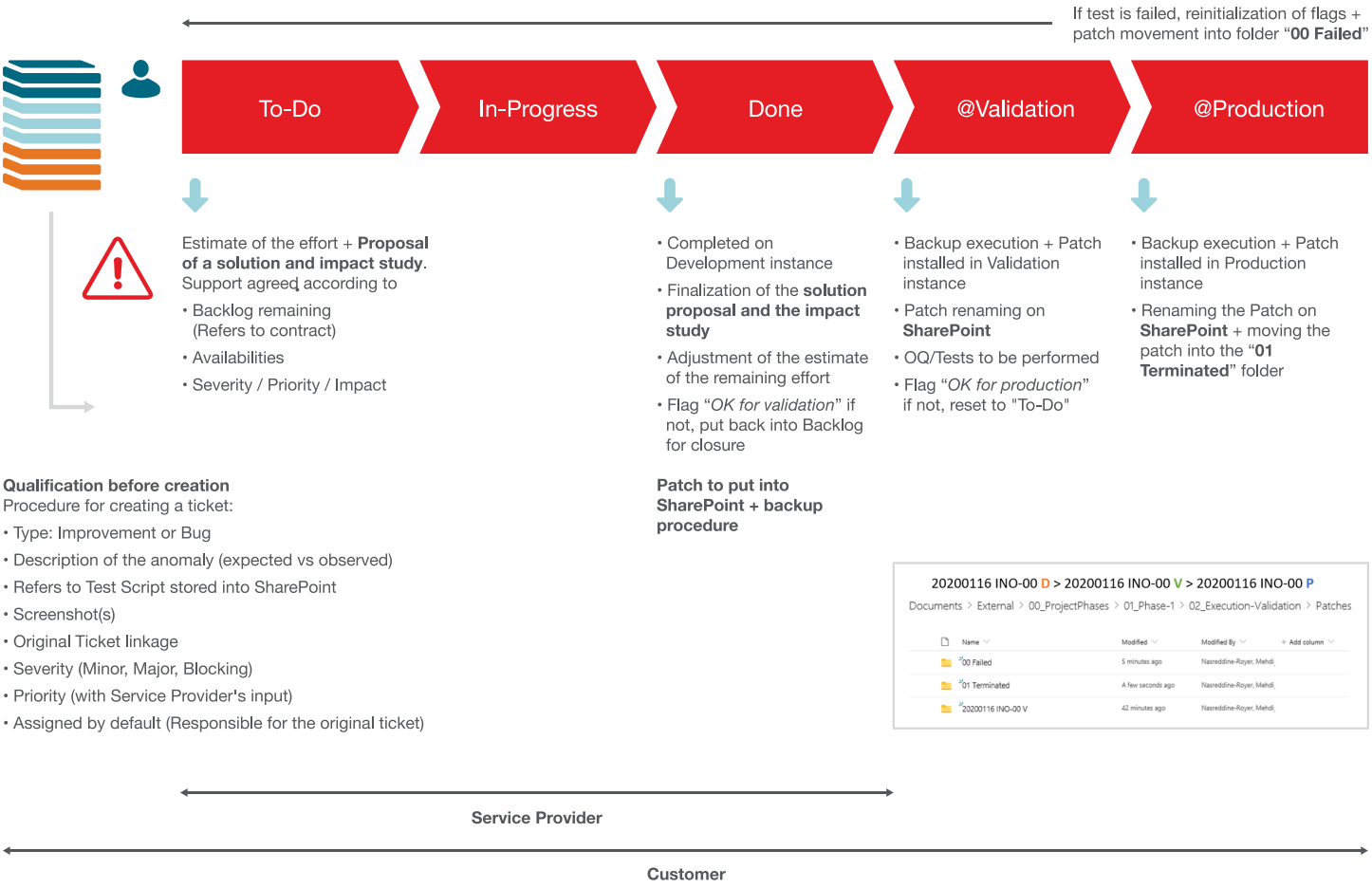
Important note: A Defect (or a Bug) is a functionality which is not compliant with the specification and reproducible.

The Tests Strategy is typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.



Change control and issue management

Stages mentioned below reflects KANBAN board of JIRA (**https://thermofisher.atlassian.net**).



IQ – Installation qualification

The IQ is about the formal assurance of the correct installation of the following systems:

- Validation System
- Production System

The scope of the IQ (for each system) will be defined in an IQ Protocol document. The following items are required to be addressed in IQ Protocols

- Standard installation
- Specific libraries to be setup
- Order of execution
- Acceptance Criteria
- Evidences (e.g. Screenshot)

The general scope of IQ activities will be as follows:

- Verification and Filing of network/hardware/software profiles for both client/server machines
- Verification that applicable standard operating procedures are in place and approved
- Verification and reporting that all applicable plans have been approved and are filed correctly
- Verification and reporting that all personnel involved in IQ activities have the correct training
- Formal execution of IQ test scripts

The IQ Scripts are under the responsibility of both sides, the Service Provider and the Customer.

OQ – Operational qualification

The OQ is about the formal assurance of the correct functional operation of the application in use. All formal OQ activities will be executed on a qualified Validation System.

The scope of the OQ will be defined in an OQ Protocol document.

The following items are required to be addressed in the OQ Protocol:

- Specific tasks (Risk Assessment's outcomes) to be tested
- Order of execution
- Acceptance Criteria
- Evidences (e.g. Screenshot)

The general scope of OQ activities will be as follows

- Verification that applicable standard operating procedures are in place and approved
- Verification and reporting that all applicable plans have been signed off and are filed correctly
- Verification and reporting that all personnel involved in OQ activities have the correct training
- Formal execution of OQ test scripts

The OQ Scripts are typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

PQ – Performance qualification

The PQ is about the formal assurance of the correct operation and use of the system from the perspective of its day to day use, and the day to day procedures used to secure and assure the validity of the data produced. Typically, formal PQ activities are executed on a qualified Production System. Test execution will be performed by trained Users.

The scope of the PQ will be defined in a PQ Protocol document.

The following items are required to be addressed in the PQ Protocol:

- Specific tasks (Risk Assessment's outcomes) to be tested
- Order of execution
- Acceptance Criteria
- Evidences (e.g. Screenshot)

The general scope of PQ activities will be as follows

- Verification that applicable standard operating procedures are in place and approved
- Verification and reporting that all applicable plans have been signed off and are filed correctly
- Verification and reporting that all personnel involved in PQ activities have the correct training
- Formal execution of PQ test scripts

The PQ Scripts are typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

Validation summary report

After the PQ report is approved the validation report can be produced. The validation summary report summarizes all validation activities. Any issues (Blocking/Major) arising from validation activities must be resolved prior to the Validation Summary Report being signed.

The Validation Summary Report must be signed off prior to the system going in Production.

The Validation Summary Report is typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

On-going system maintenance

It is essential that validated systems be kept in a compliant state after the validation report is signed off and the system has gone live. To achieve these system maintenances, procedures will be modified / developed by the project team with help and support of the Service Provider.

- Operational plans and procedures
- Training
- Problem management and resolution
- Service Level Agreements (SLAs)
- System management
- Backup and recovery
- Configuration management
- Operational change control
- Security management
- Performance monitoring
- Record retention, archiving and retrieval
- Business continuity planning
- Periodic review and evaluation
- System retirement

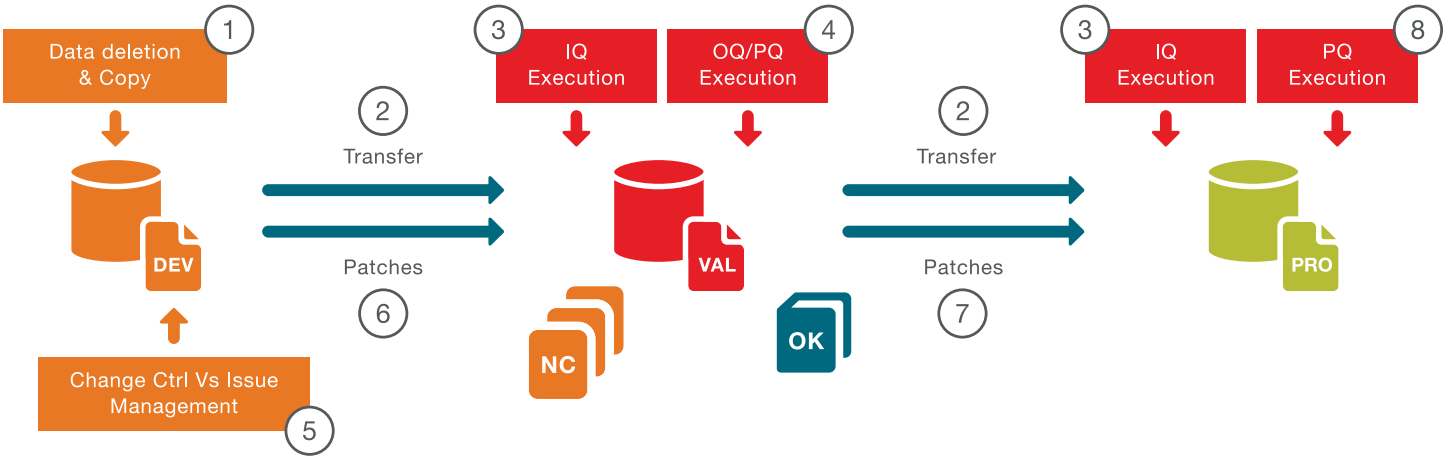
The system maintenance procedure and/or modifications to existing system-maintenance related procedures will be completed prior to the system going in Production.

The Maintenance Procedures are typically under the responsibility of the Customer (or third party) unless stated otherwise in the Contract (e.g. Statement of Work). Service Provider can also help and support.

thermoscientific

Strategy of validation / production transfer

Process to be applied to transfer patches between Development > Validation > Production.



1. Preperation of the Development before transfer
2. Transfer of objects from Development to Validation / Production
   - Delete dynamic data thanks to data deletion script performed in Development – Make a Backup first
   - Backup / copy of the SQL instance + Files
3. Execution of IQ Scripts
4. OQ / PQ execution
5. Change Control and Issue Management – managed by JIRA
6. Transfer of patches from Development to Validation (after getting approval)
7. Transfer of patches from Validation to Production (after getting approval)
8. Go-Live & PQ execution

Find out more at **thermofisher.com/digitalscience**

ThermoFisher SCIENTIFIC