APPROVAL

Role	Name	Function	Signature
Author	Evmorfia Kilimtzidi	QA&SA	
Review	Mauro Rinaldi	RAQM	
Approval	Mathieu Horras	CEO	

PURPOSE

This procedure describes the methodology used by ASPIVIX SA to control the software tools used to meet the requirements of EN ISO 13485:2016 (Clause 4.1.6).

SCOPE

This procedure applies to any computer software used in the quality management system (e.g., ERP, QMS software, LIMS, complaint handling tools, document control, electronic signatures) that must be validated prior to initial use and re-validated when changes occur. Records of validation activities must be maintained.

RESPONSIBILITIES

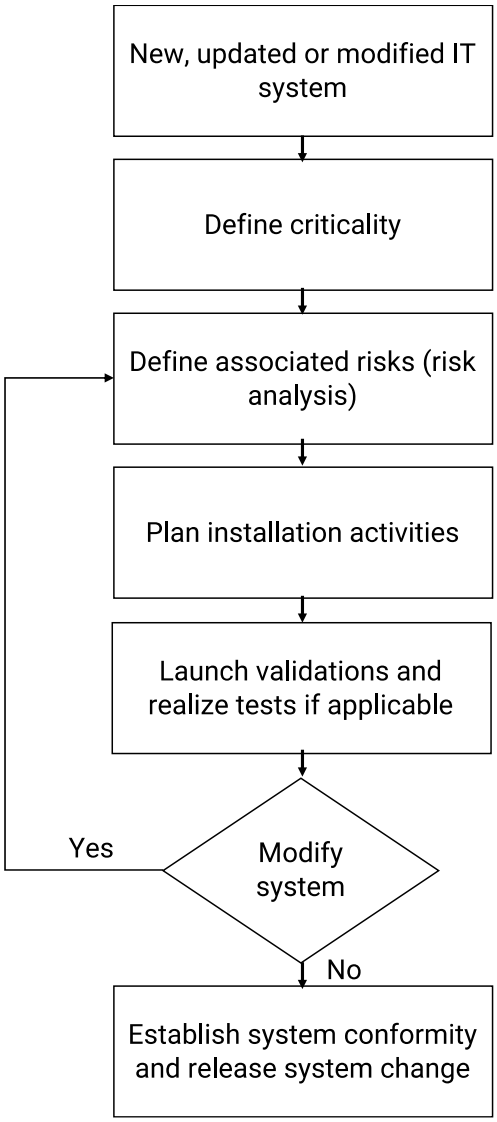
Responsible for established, implementing and maintaining this SOP is the Regulatory Affairs and Quality Manager.

DOCUMENT HISTORY

Description of Changes	Version
Initial version	A
Update risk assessment criteria and category of IT system/SW + tool kit “Adobe Sign Validation Pack for Electronic Signatures" + details on reporting and revalidation	B
Update to clarify that this INS pertains specifically to software tools to avoid confusion with SOP-208 Software Development	C

TABLE OF CONTENT

1 PROCEDURE FLOWCHART

Actions	Who?	Comments
	Department Responsible RAQM/ Department Responsible RAQM/ Department Responsible RAQM/ Department Responsible RAQM/ Department Responsible RAQM/ Department Responsible RAQM RAQM	Responsible for every department must inform the RAQM when a new software is to be used or when a software is to be updated or its version modified. The use of the T-206-1 enables to list: - The software with their criticality, their class and their version. - If necessary, the modules with risk levels and validation protocols followed - If necessary, the planning elements for every module. - The validation status - The modifications identification In case of IQ, OQ and/or PQ validation to performed ➔ a qualification report based on T-200-15 is used for recording the verification and validation. Note: For the Adobe Sign platform, the dedicated “Adobe Sign Validation Pack for Electronic Signatures” provided by Adobe Sign and Montrium is used. The RAQM updates the T-206-1.

2 PROCEDURE DESCRIPTION

2.1 CATEGORIES OF SOFTWARE / IT SYSTEM

- Quality management software (GED, excel tool such as CAPA follow up, supplier evaluation follow up, …)
- Software used for Design/Production management and service delivery (CAD, GPAO, ERP, SCADA Supervisory control and data acquisition) for production, ...)
- Software used for monitoring and measurements (GMAO, metrology software, excel tool MME follow up, …)

2.2 SYSTEM CRITICALITY DEFINITION

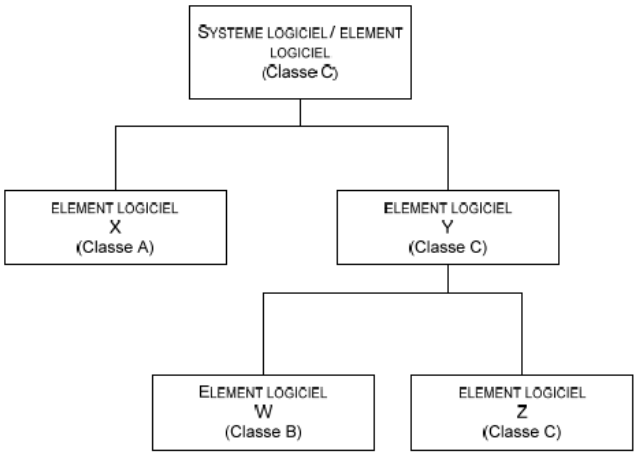
Depending on the criticality of the system, the following validation method will be applied:

Criticality level	Patient/product risk Regulatory risk	Validation Method to follow
C (Major)	Direct impact on product performance or patient safety (serious adverse event) or Direct impact on regulatory compliance of the Quality Management System.	- Complete validation: IQ, OQ, PQ - Saving the version, - Staff training verification.
B (Moderate)	Indirect impact on the product performance or patient safety (non-serious adverse event or reversible event) or Indirect impact on regulatory compliance of the Quality Management System.	- Verification by the realization of a qualification report to demonstrate that the functionalities used comply with the requested specifications (such as systematic backward compatibility test). - Saving the version, - Verification of staff training.
A (Minor)	No impact on the product performance or patient safety Or No impact on regulatory compliance of Quality Management System.	- Saving the version, - Staff training verification.

2.3 MODULAR ARCHITECTURE DEFINITION

A modular architecture can be realized for complex systems, in case where modules do not have the same criticality level. In this case, the criticality will be assessed and scored for each and every module.

Example of modular architecture:



If the overall system is justified in criticality level C (critical), the subsystems can be classified in A, B or C. It is important to justify the level of each module/subsystems, after having justified the class of the overall system.

2.4 VERIFICATION / VALIDATION PROTOCOL DESIGN

VALIDATION
The validation protocol depends on the system criticality.
The extent of the validation must be proportionate to the risks associated with the use of the software.

For the critical systems, an IQ, OQ, PQ approach is preferably used.
The minimum IQ content includes:

- The suppliers' documents review
- The training of operators
- The review of the installation pre-requisites and the implementation of those pre-requisites
- Parameters set-up, etc.

The minimum OQ content includes:

- Used functionalities verification
- System limits and worst cases use scenario verification
- Alarms and error messages tests
- Control system tests

The minimum PQ content includes:

- Test all use scenarios and measure the reliability, robustness, transfer times, display response time, etc.

VERIFICATION
When applicable (according to §2.2), a verification of software/IT system consists of the following steps:

- Verification protocol,
- Verification report including the demonstration that the functionalities used comply with the requested specifications.

The release of the software / IT system can only be done once verification has been performed.

Verification/validation must be related only to the functionalities/features of the software which have an impact on the QMS.

Reporting:

- Verification/validation are recorded on template T-200-15 (Qualification Report).
- Specifically for Adobe Sign platform (electronic signature software), the validation is reported on dedicated Adobe Sign validation pack provided by the supplier.

2.5 VALIDATION LAUNCH

The validation launch is piloted by the RAQM.
The responsible person for the IT System defines the test validation protocols.
"Key users" performs the tests (current of future system users).

2.6 REVALIDATION IN CASE OF UPDATE OR MODIFICATION OF THE SYSTEM

The RAQM in relation with the manager of the concerned department identifies the changes and evaluates the impact of the changes (proportionally to the risk) and finally defines the magnitude of the re-validation/re-verification accordingly to the risk management. The revalidation can be partial or total according to the analysis performed with technical support if necessary.
The changes are recorded in the template T-206-1 software validation follow-up.

2.7 CONFIGURATION

When applicable, the IT systems developed internally will be traced according to the following mode:

Version X.Y.Z

X = main version (modified in case of major change)
Y = secondary number changed in minor change box
Z = modified number in case of minor debugging.

In case of excel calculation formulas, the revision of the template will be used for tracking the change.

3 REFERENCES

3.1 PROCEDURES, INSTRUCTIONS AND GUIDELINES

SOP-206 Validation Activities

3.2 TEMPLATES AND FORMS

T-206-1 Software Validation Follow-up
T-200-15 Qualification Report

Aspivix SA | Route de la Corniche 8 | Bureau 10 | 1066 Epalinges | Switzerland

Certificate of Completion

INS-206-1-rev.C_Software_Validation_clean.pdf

Printed on 2025-09-01 - 14:00:54 UTC

Document Details

Created by: Eva Kilimtzidi
Created on: 09/01/2025 08:59:31 (UTC)
Creation IP Address: 185.10.224.50
Signers: 3

Document ID: 606
Signature:
38733e15fe34b1c8d3e5de7a0e5ac775cfc4771d98cd384fac0f92d6d8e07afe

Participants

Signatory	Email	Email Verification
Eva Kilimtzidi	eva.kilimtzidi@aspivix.com	☑
	Signatory's hash:	3f97903ae565a14bf4e557f31bdd2ec328d3445986c10e6a735937942aa50b68
Mauro Rinaldi	mauro.rinaldi@aspivix.com	☑
	Signatory's hash:	78638443ccaea43979b1606b4de42a2f233d7b2ddc5d3d6ea75d60850cc12138
Mathieu Horras	mathieu.horras@aspivix.com	☑
	Signatory's hash:	83aef1e3f340e4bb80e3e4cb135d147b2d8f2a1fb0e3e2072f3ce586ce4786c8

Email Verification: The signatory has confirmed control of their email inbox by clicking on a unique link

Signing Events

Action	By	Date (UTC)
Creation	Aspivix SA, Eva Kilimtzidi eva.kilimtzidi@aspivix.com	09/01/2025 08:59:31
	Signature:	38733e15fe34b1c8d3e5de7a0e5ac775cfc4771d98cd384fac0f92d6d8e07afe

Action	By	Date (UTC)
Signature 	Aspivix SA, Eva Kilimtzidi eva.kilimtzidi@aspivix.com	09/01/2025 08:59:37
	Signature: e9b059b4889ea61344e491289592c3e23e2cc8c7d2c0b65b7cb5b355116ff81f	
Signature 	Aspivix SA, Mathieu Horras mathieu.horras@aspivix.com	09/01/2025 08:59:59
	Signature: a4a87787fe334f7c8e3f9cdfcded0b7f12635c2f1a48d4d4b8e6866a83aaec85d2	
Signature 	Aspivix SA, Mauro Rinaldi mauro.rinaldi@aspivix.com	09/01/2025 14:00:53
	Signature: 049696215deaea59720ac9287d0589628898a18d801c96eae851f81d0835ad97	

✔ The document's integrity is valid.

The final document and this completion history have been sent by email on 09/01/2025 to: mauro.rinaldi@aspivix.com, mathieu.horras@aspivix.com, eva.kilimtzidi@aspivix.com.

Access Logs

Viewed/downloaded by	Date (UTC)	State
Aspivix SA, Eva Kilimtzidi eva.kilimtzidi@aspivix.com	09/01/2025 08:59:32	Before Signature
Aspivix SA, Eva Kilimtzidi eva.kilimtzidi@aspivix.com	09/01/2025 08:59:33	Before Signature
Aspivix SA, Mathieu Horras mathieu.horras@aspivix.com	09/01/2025 08:59:47	Before Signature
Aspivix SA, Eva Kilimtzidi eva.kilimtzidi@aspivix.com	09/01/2025 09:19:50	Before Signature
Aspivix SA, Mauro Rinaldi mauro.rinaldi@aspivix.com	09/01/2025 14:00:48	Before Signature
Aspivix SA, Mauro Rinaldi mauro.rinaldi@aspivix.com	09/01/2025 14:00:49	Before Signature

Aspivix
Route de la Corniche 8
1066 Epalinges | Switzerland

contact@aspivix.com
https://aspivix.com

Tax ID: CHE-347.247.288 TVA
HRB Nr: