	Standard Operating Procedure (SOP)	
	SOP-279	Page 1 of 33
	Computerized System Qualification and Validation	

1 PURPOSE

This procedure defines the process by which GxP computerized systems used at AveXis are validated to assure they meet their intended use and that all regulatory requirements are satisfied following the computerized systems life cycle phases:

- Initiation and System Identification
- Requirements Gathering and Design
- Implementation and Testing
- Operation and Maintenance
- Decommissioning/Retirement

Validation of computerized systems provides a high degree of assurance that the system will perform as expected in accordance with its predetermined specifications and user-defined requirements.

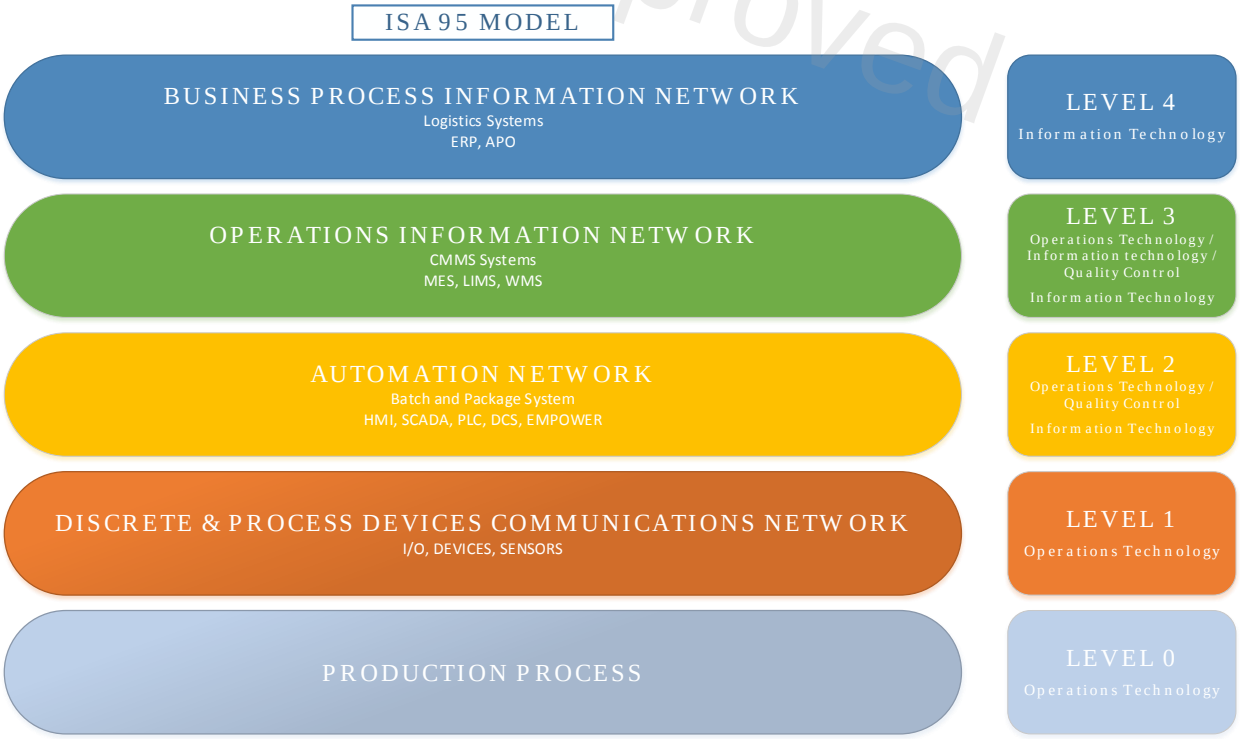
2 SCOPE

This procedure applies to new and existing computerized systems used for GxP operations at AveXis.

IT solutions that are identified as GxP will follow this procedure.

Infrastructure with GxP applications and GxP solutions will follow this procedure.

Level 2 system servers and application installation will follow this procedure. For components of the Level 2 systems connected to Level 1 equipment, SOP-035.



Out of scope are qualification of production and laboratory equipment - which follow SOP-037, *COTS Equipment Commissioning*, and SOP-035, *Commissioning and Qualification*. For automated manufacturing equipment or laboratory equipment, computer system specification and verification must be part of an integrated systems approach to ensure compliance and fitness for intended use of the complete system. Separate computer system validation is not required.

The maintenance of computerized system controls such as access control (user and security access management), configuration and backup management, and all other required operational procedures noted in Section 8.2.6 must be addressed in the qualification documents.

3 ROLES AND RESPONSIBILITIES

Functional Area/Role	Responsibility
General Considerations	• Several of the roles may be combined except for the Quality Assurance role. If multiple business processes or organizational units are supported by a system, then multiple individuals may be assigned to the roles. • All documents generated as part of computerized systems life cycle will follow the appropriate approval process by affecting stakeholders. Refer to responsibilities' matrix defined in Appendix A. Other responsibility matrix can be employed provided it is defined in the Validation Plan and approved by QA.
Business Process Owner	• The BPO is ultimately accountable for ensuring that the computerized system and Quality Systems supporting the business process are in compliance with AveXis requirements and are fit for the intended business process. • The BPO is a member of the business with process knowledge to own the data/records in the system related to their business process. There may be multiple BPOs that use a computerized system; one BPO may also be the System Owner (e.g. local Asset Centre). • Takes operational responsibility for the computerized system throughout its life cycle and ensure that the system is fit for intended use. • Ensures applicable processes and procedures are in place, and that retention requirements are adhered to. • Reviews and approves specified deliverables generated during the validation process. • Ensures the availability of training materials and that users are trained properly. • Releases the computerized systems with Quality Assurance, as appropriate
System Owner	• Represents the needs of the business users and the BPOs. There is only one SO for each computerized system and that individual is the single point of contact for the computerized system. The SO may delegate responsibilities to a person within the business as required but they retain overall accountability for the validated status of the computerized system. • Ensures the availability, installation, maintenance, and support of the system throughout the validation life cycle. • Establishes and maintains the validated state of the system. • Collects and tracks system errors. • Ensures the integrity of records residing on the system. • Initiates and manages change control for the system. • Ensures data validity and compliance throughout the life cycle of the system. • Reviews and approves access requests for the system. • Reviews and approves specified deliverables generated during the validation process. • Ensures a backup and restore process is available for the system.

Functional Area / Role	Responsibility
Validation (Quality Manager)	• Validation is accountable for the development of the validation plan and adherence to it. Validation ensures that the project deliverables have been authored, reviewed and approved accordingly, and oversees the testing processes within the project. Validation ensures that project processes such as project change, document and configuration management are established and followed. • Responsible for validating the computerized systems according to this procedure. • Authors and / or provides input to the contents of the specified deliverables during the validation life cycle, including system specifications, test qualification protocols and/or reports to ensure AveXis technical requirements are met. • Prepares meeting minutes for meetings related to validation activities, tracks validation action items, and tracks resolution of any issues. • Assists the System Owner and Business Process Owner in the development of training materials and/or SOPs on the use and operation of the computerized system, as necessary. • Assists with Pre-Qualification related documents. • Collaborates with trained personnel to assist in testing of the computerized system, as necessary. • Leads the execution of validation activities and reviewing results. • Owns the periodic review / periodic requalification program and schedule. • Validation may also be known as the Validation SME, Quality Manager (QM), Project Quality Manager (PQM), Operational Quality Manager, or another similar name.
Quality Assurance (QA) / QA e-Compliance Responsible Person (as applicable) to EU GDP	• The QA/QA e-Compliance function is accountable to ensure that the computerized system and the associated support processes meet the expectations defined in the Quality Manual. QA e-Compliance is accountable to provide the quality oversight for validation of new GxP applications and for the life cycle of the entire GxP computerized system portfolio. With respect to CSV, the QA/QA e-Compliance person liaises with, represents, and is the single point of contact for, the business QA functions who may work with the computerized system on a day-to-day business. • Performs independent review and approval of validation life cycle activities to ensure adherence to relevant GxP requirements and procedures. • Provides regulatory guidance and recommendations for specified deliverables generated during the validation life cycle of the computerized systems. • Formally releases the validated computerized system for use in the intended operating environment. • This role reports to the Quality Assurance organization. Other quality functions can provide quality oversight provided training has been completed per this SOP.

Functional Area/Role	Responsibility
System User Groups	• Subject Matter Expert on the business process. • Assist with system operation during validation activities. • Responsible for working with the system during operational usage within approved procedures. • Assist in system training as applicable.
Application Manager (AM)	• The AM (may also be known as the System Infrastructure Provider or Administrator) is responsible for oversight of the day-to-day operation of the computer system and ensures the supporting processes defined in the SOP are in place and being followed. This is a technically knowledgeable person who is accountable for ensuring that service agreements with the business are met. • Provides the System Infrastructure necessary to run the system • Supports in the installation and maintenance of the computerized system during the complete system life cycle. • Provides service level support to system owner. • Maintains access rights for the system covering account creation, modification and deactivation. • Supports in system development and configuration. • Supports in master data development and configuration. • Implements changes described in the change controls. • Conducts periodic review of the user access rights. • Maintains system administration records. • Performs backup and restore of the system as applicable. •
System Supplier	• Provides system application and support in the development and maintenance of the system as applicable. • Provides service level support and upgrades as applicable. • Conforms to the quality agreement.
Subject Matter Expert (SME)	• The SME is a general role that can represent multiple domains and is involved at every stage of the lifecycle of the CS to provide specification knowledge required to fulfill validation and operation activities. Different SMEs may be involved into different validation activities, based on their special expertise. This role for example is covered by Business QA, Security Engineers, and Technical Writers.

4 SAFETY AND GENERAL INFORMATION

Not Applicable

5 EQUIPMENT AND MATERIALS

Not Applicable

6 REFERENCES

Document/Reference	Title/Description
2013/C 343/01	EU Guidelines on Good Distribution Practice of Medicinal Products for Human Use
21 CFR Part 11	Code of Federal Regulations Title 21, Part 11 Electronic Records & Electronic Signatures
EudraLex Volume 4 Good Manufacturing Practice	Annex 11 Computerized Systems
FDA Guidance for Industry	Data Integrity and Compliance with cGMP - Guidance for Industry
GAMP 5	A Risk-Based Approach to Compliant GxP Computerized Systems
MHRA	MHRA GxP Data Integrity Definitions and Guidance for Industry
POL-006	GxP Record Retention
POL-007	Data Integrity
POL-012	User ID and Electronic Password Policy
POL-017	Computerized System Life Cycle
POL-019	Backup and Restore Policy
POL-022	IT Infrastructure Policy
SOP-003	Good Documentation Practices
SOP-004	Change Control System Overview
SOP-005	Non-Conformance and CAPA System
SOP-034	Engineering Design Review
SOP-035	Commissioning and Qualification
SOP-037	COTS Instrument and Equipment Qualification
SOP-041	Computerized Systems Risk Assessment
SOP-042	Supplier Audits
SOP-045	Supplier Selection and Qualification
SOP-238	Data Integrity Controls
SOP-362	Site-Specific Data Retention
SOP-411	Electronic Records and Electronic Signatures
SOP-418	Periodic Review of Computerized Systems
SOP-480	Computerized System Data Integrity Assessment

Document/Reference	Title/Description
SOP-555	System Impact Assessment
SOP-632	Validation Exception Record
SOP-1018	Validation Master Plan and Inventory for GxP Computer Systems
SOP-1187	Supplier Quality Management of GxP Computerized Systems
FORM-218	Validation/Qualification Exception Report Form
FORM-355	System Impact Assessment Form
TEMP-031	Validation Summary Report Template
TEMP-129	User Requirements Specification Template
TEMP-142	Data Integrity Assessment
TEMP-144	Periodic Review of Computerized Systems Template
TEMP-145	Protocol Template for Installation/Operational/Performance Qualification (System)
TEMP-146	System Specification Template
TEMP-147	Traceability Matrix Template
TEMP-148	Validation Plan Template
TEMP-149	Risk Assessment Template
TEMP-151	Protocol Report Template
TEMP-162	Validation Plan Summary Report Template
TEMP-323	Computer System Classification
WI-276	Computer System Content Scaling

7 ABBREVIATIONS AND DEFINITIONS

Term/Abbreviation	Definition
ACE	Adaptive Compliance Engine – AveXis electronic document management system.
ALCOA+	This is a term used to describe that data should be Attributable, Legible, Contemporaneous, Original, and Accurate throughout its lifecycle. The Data should be complete, available, consistent, and enduring.
AM	Application Manager
AP	Archival Plan
AR	Archival Report
BC	Business Continuity
BCP	Business Continuity Plan
BPO	Business Process Owner
BSO	Business System Owner
Computer or Computerized System (CS)	Hardware, system software (e.g., operating systems, databases, etc.), application software, peripheral devices, and supporting documentation.
Computerized System Validation (CSV)	Documented evidence which provides a high degree of assurance that a system or process consistently meets its predetermined specifications and quality attributes.

Term/Abbreviation	Definition
Configuration Management	The process of identifying and defining the configuration items in a system, controlling the release and change of these items throughout the system life cycle, recording and reporting the status of configuration items and change requests, and verifying completeness and correctness of the configuration items.
Configuration Specification (CS)	A document that specifies how the system is configured; describing the arrangement and interconnections of its constituent parts as well as its configured settings. The Configuration Specification identifies configuration parameters, settings and supporting file / scripts.
COTs	Commercial-Off-The-Shelf
CR	Code Review
DCMP	Data Conversion / Migration Plan
DCMR	Data Conversion / Migration Report
DQ	Design Qualification
DR	Disaster Recovery
DRP	Disaster Recovery Plan
DRR	Disaster Recovery Report
Design Specification (DS)	A document that specifies a detailed description of the modules or components and includes the software design emphasizing any custom code and configurations for the system or system components.
ER/ES	Electronic Records / Electronic Signatures
Functional Specification (FS)	A document that specifies the functions that a system or component must perform to ensure it meets the user needs as described in the URS.
FRA	Functional Risk Assessment
GAMP	Good Automated Manufacturing Practice
Harm	Damage to health, including the damage that can occur from loss of product quality or availability. Harm is the result or outcome of a hazard. This term is used to mean damage to consumer health or reduction in product quality. Example: The warehouse is destroyed / damaged by fire incurring loss of product, repair costs and reduced availability for distribution.
Infrastructure	Infrastructure includes facilities, computer network components, servers, operating systems, layered software (e.g. middleware, database managers, and desktops packages), peripherals, personal computers, mobile computing, and related procedures and records.
IM	Incident Management
Installation Qualification (IQ)	Documented verification that all important aspects of hardware and software installation adhere to the computerized system specification and/or manufacturer's recommendations. IQ may also be referred to as Installation Verification (IV).
Operation Qualification (OQ)	Documented verification that the system operates in accordance with the computerized system specification throughout all anticipated operating ranges. OQ may also be referred to as Operation Verification (OV).

Term/Abbreviation	Definition
OT	Operational Technology
Performance Qualification (PQ)	Documented verification that a computerized system performs its intended functions in accordance with user requirement specifications when used in its normal operating environment. Performance Qualification is sometimes referred to as User Acceptance Testing (UAT).
PrM	Problem Management
PVR	Periodic Validation Review
QAA	Quality Assurance Agreement
QA eCPL	QA eCompliance
QM	Quality Manager
RP	Retirement Plan
SaaS	Software-as-a-Service – the provision of a software solution where vendors manage data, middleware, servers and storage as well as installing, managing, and upgrading software.
SLCD	System Lifecycle Deliverable
SME	Subject Matter Expert
SQM	Supplier Quality Management
SW	Software
TSO	Technical System Owner
TSP	Test Strategy & Plan
TSR	Test Summary Report
Traceability Matrix	A document that traces the user requirements, system design, and testing through to the documentation where the requirements are verified.
UAT	User Acceptance Test
User Requirements Specifications (URS)	A document which defines the intended use of a computerized system as determined by the end user of the system.
VMP	Validation Master Plan
Validation Plan (VP)	A document which defines the validation activities and how they will be performed. It also describes the responsibilities.
Validation Plan Summary Report (VR)	A document that summarizes activities specified by the Validation Plan and lists all deliverables generated during the validation process. The Validation Plan Summary Report also summarizes the conclusion regarding the suitability of the system for intended use.

8 PROCEDURE

8.1 General Concepts

A computerized system is defined as consisting of software and hardware, and peripheral devices together with the supported business processes and associated documentation.

8.1.1 A computerized system is developed, operated, maintained and retired according to the validation life cycle phases:

- Initiation and System Identification
- Requirements Gathering and Design
- Implementation and Testing
- Operation and Maintenance
- Decommissioning/Retirement

An inventory list of computerized systems that are GxP applicable shall be available and maintained in a computerized system inventory list. See SOP-1018 for instructions and responsibilities.

Each system should be uniquely identified by assignment of unique system number.

Changes to GxP computerized systems including implementation, modification (i.e., upgrades, repairs), retirement/decommissioning should be documented per applicable change procedures. Depending on the scope and impact of the change, an abbreviated list of activities/documentation is acceptable. Partial or full validation/qualification is acceptable based on scope of change and impact.

When there is a change to an existing legacy system, existing documentation can be revised to reflect the change. The existing documentation does not need to be updated or revised to the latest document format.

The scope and extent of validation activities should be based on intended use, risk and complexity of the system.

All system life cycle documentation may not be applicable to all systems. Documentation may have a combination of content elements intended to satisfy requirements for multiple document types as long as the required content or approval are met.

The Validation Plan (VP) can be used to describe the validation strategy, documentation deliverables, and roles and responsibilities differing from the process defined in this procedure provided the specific strategy is defined in the Validation Plan and is approved by QA.

8.2 Validation Life Cycle Phases

8.2.1 Initiation and System Identification Phase

During this phase, the need for a computerized system (either to replace an existing manual process or to replace an existing computerized system) is determined.

The documents to be developed and activities to be completed are described below:

8.2.1.1 Computer System Classification (CSC) and System Impact Assessment

8.2.1.1.1 For IT solutions the computer system classification will be used. Complete the CSC with the correct stakeholders will determine key governance, security and compliance risks, and the overall system classification. Complete the classification using TEMP-323. Novartis integrate IT solutions utilizing a High Level Classification and Consultation (HLCCD) tool following SOP-8027419 will be accepted as an equivalent Computer System Classification. For non-IT solutions, SOP-555 will be used to assess system impact. The system validation plan will explain equivalency to GxP High, Medium, or Low.

8.2.1.1.2 This process classifies the following areas for computer systems:

- Confidentiality
- Integrity
- Availability
- Data Privacy
- GxP
- SOX

8.2.1.1.3 In addition to the classification, the impact assessment also documents the following information:

- General system information, including system description and supported business process(es).
- Whether the system is externally supported or hosted – this is used to identify applicable Third Party controls.
- Types of records stored by the system – this issued to ensure records retention requirements are identified.
- System quality approach and where lifecycle documents will be stored – this is to support assessment and any future updates required.

8.2.1.1.4 Determine the system's Information Confidentiality. The system information classification must align with the highest confidentiality classification of business information the system holds, manages, or processes.

Classification	Confidentiality Description
Strictly Confidential	Strictly Confidential Business Information is the most sensitive information, the disclosure of which would cause severe and serious damage to AveXis. Such damage could include financial losses, damages to the AveXis brand and reputation, or legal actions or prosecutions against AveXis.
Restricted	Restricted Business Information is very sensitive information, the disclosure of which would cause significant or substantial damage to AveXis. Such damage could include

Classification	Confidentiality Description
	financial losses, damages to AveXis brand and reputation, or legal actions or prosecutions against AveXis.
Business Use Only	Business Use Only Business Information is information used in the normal course of AveXis business to support business activities. In case of loss or disclosure it would cause some damage to the interests of AveXis. This is the default Classification level.
Public	Public Business Information is information that is approved by AveXis management to be made available to the public.

8.2.1.1.5 Determine the system's Integrity.

Classification	Integrity Description
Vital	Systems are classified as Vital if accidental or malicious alteration of hosted, stored or managed Business Information would cause serious damage to the point of endangering the existence of AveXis. This is typically information that: • Is subject to high impact fraud • If accidentally or maliciously altered, could results in serious operational mistakes threatening health and safety of people using AveXis products. • If accidentally or maliciously altered, could result in wrong strategic decisions by Management
Standard	Systems are classified as Standard if accidental or malicious alteration of hosted, stored or managed Business Information would cause less than serious harm to the interests of AveXis. This is the default Classification level.

8.2.1.1.6 Determine the system's Availability.

Classification	Availability Description
High	Availability High applies to systems for which operational unavailability for more than 24 hours has a high business impact. In general these are systems for which the maximum tolerable unavailability time is less than 1 day (or less than 1 hour).
Medium	Availability Medium applies to systems for which operational unavailability for more than 24 hours has a significant business impact.

Classification	Availability Description
	In general these are systems for which the maximum tolerable unavailability time is 1-5 days.
Low	Availability Low applies to systems for which operational unavailability for more than 24 hours has a minor business impact. In general these are systems for which the maximum tolerable unavailability time is more than 5 days and recovery is "best effort". This is the default Classification level.

8.2.1.1.7 Determine the system's Data Privacy

Category	Data Privacy Description
Sensitive Personal Information (SPI)	Sensitive Personal Information is a subset of Personal Information that requires a higher level of protection. Such information may include racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, social security or insurance information, criminal charges, conviction / sentence, or a person's sexual orientation, or health information. Data elements that make up Sensitive Personal Information may vary by country and local law should be consulted. Associates should check with their Data Privacy Business Partner for guidance. Health information is always considered as Sensitive Personal Information at AveXis.
Personal Information – Full (PI Full)	Personal Information Full means all information that relates to a person (aka 'data subject') where that person can be identified by you or others. In some cases, the person can be identified directly (e.g., by name or photograph) or the person can be identified indirectly (e.g., a medical insurance number, position in a company or by means of a study code assigned in a clinical trial). In some countries, Personal Information may also include information such as medical device serial numbers, biological samples, IP addresses or information relating to a company ("legal person"). Associates should check with their Data Privacy Business Partner for guidance. Personal Information Full is information that is more than a simple identifier or (business) address book contact data, but is not classified as Sensitive Personal Information.
Personal Information – Limited (PI-Limited)	Personal Information Limited is information solely used for the purpose of authentication and / or access / role management, such as 5.2.1 / Unique ID, Active Directory data (e.g. AveXis email address, employee name, employee title, function, division, or AveXis address or contact information).

Category	Data Privacy Description
	Where this information is collected for purposes different to just giving access to an Information System, Data Protection Officer consultation is required to confirm the Data Privacy classification.
N/A	This is the default Classification level, which indicates no personal identifiable information.

8.2.1.1.8 Determine the system's GxP Classification.

GxP Category	GxP Level Description
GxP – High	Business process has a direct impact on Patient Safety because it is a: • Process to manage clinical studies (protocols, patients, treatments, clinical drug manufacturing or supply and associated records supporting this business process). • Process for handling adverse events, complaints, pharmacovigilance, prost-market surveillance, product recall or product withdrawal and associated records supporting this business process. Or – Business process has a direct impact on Product Quality because it is a: • Process for specification, detection, verification, control or correction product or product ingredients quality (raw material, intermediates, drug substance, excipient, drug product) (like in-process, goods receipt, QC) and associated records supporting this business process. • Process for commercial product manufacturing and associated records supporting this business process. • Drug supply chain or distribution process ensuring product availability on the market and associated records supporting this business process.

GxP Category	GxP Level Description
GxP – Medium	Business process has an indirect impact on Patient Safety because it is a: • Supporting process to manage clinical studies (protocols, patients, treatments, clinical drug manufacturing or supply) and associated records supporting this business process. • Supporting process for handling adverse events, complaints, pharmacovigilance, prost-market surveillance, product recall or product withdrawal and associated records supporting this business process. Or – Business process has an indirect impact on Product Quality because it is a: • Supporting process for specification, detection, verification, control or correction product or product ingredients quality (raw material, intermediates, drug substance, excipient, drug product) (like in-process, goods receipt, QC) and associated records supporting this business process. • Supporting process for commercial product manufacturing and associated records supporting this business process. • Supporting process drug supply chain or distribution process ensuring product availability on the market and associated records supporting this business process.
GxP – Low	Business Processes and records are regulated (GMP, GCP, GLP, GDP, submission or other) but are not supporting processes for Patient Safety or Product Quality (as outlined above).
N/A	This is the default Classification level, which indicates which indicates that the system supports a business process that is not subject to GxP.

8.2.1.1.9 Determine if the system has SOX relevant information.

SOX Assessment	
SOX	Sarbanes-Oxley (SOX) systems host Business Information in scope of the Sarbanes-Oxley Act, and support AveXis Financial regulated processes.
N/A	This is the default Classification level, which indicates that system is not SOX relevant.

8.2.1.1.10 Completing the system impact assessment.

8.2.1.1.11 Based on the GxP classification, scaled validation activities and CSV deliverables content creation or update shall be identified, planned according to principles defined in this procedure and documented in the Validation Plan.

8.2.1.1.12 The GxP classification obtained (High / Medium / Low), shall be used to

- Identify the minimum and, if applicable conditional GxP validation activities and CSV deliverables, WI-276.
- Identify authoring and signing role for each CSV, see Appendix A.

8.2.1.1.13 Validation activities are executed and CSV generated or updated according to VP or change documentation. If deviations from this procedure and individual plan occur, these shall be aligned with the corresponding approvers, documented and reported.

8.2.1.2 Validation activities, CSV output, phasing, scaling, and main responsibilities for the main elements are shown in the figure below:

Figure 1: CSV Phases, Deliverables, Scaling, and Ownership

Phases	Responsible	Activities	CSV Output	Scaling
Requirements / Specifications	Validation / QM	Scale SLCD / Plan Validation	Validation plan (VP)	Mandatory
	BPO / BSO	Gather Requirements	User Requirements Specification (URS)	Mandatory
	QA	Manage Supplier Quality	Assessment	Conditional
	TSO	Specify System	Functional Specification (FS) / Configuration Specification (CS) / Design Specification (DS)	Scaled
	Validation / QM	Assess Functional Risk	Functional Risk Assessment (FRA)	Scaled
Design / Build	TSO	Review Custom Code	Code Review	Conditional
	TSO	Traceability Matrix	Trace Matrix	Mandatory
Verification / Test	TSO	Verify / Test	Installation Qualification (IQ)	Scaled
			Operation Qualification (OQ)	Conditional
	BSO	Verify / Test	Performance Qualification (PQ)	Mandatory
Release	BSO	Report Validation	Validation Report (VP)	Mandatory

8.2.1.3 System Identification Number

System identification number should be assigned during this phase.

8.2.1.4 Data Integrity Assessment

A data integrity assessment should be performed for systems used for data collection, data control, data acquisition, data processing, reporting, electronic records, electronic signatures and audit trails in accordance with SOP-480, Computer System Data Integrity Assessment. A data integrity assessment shall be performed and completed at any time before the Validation Plan Summary Report has been approved.

8.2.2 Requirements Gathering and Design Phase

This phase describes the requirements gathering and design phase for the life cycle.

The documents to be developed and activities to be completed are described below.

8.2.2.1 User Requirements Specification (URS)

The URS should be developed to define the intended use of the computerized system as determined by the end user of the system and should be traceable to the business process. Requirements for security, 21 CFR Part 11 (electronic records & signatures), audit trails, operation usage, interfaces, backup and restore, and data reporting should be evaluated. In addition, the business process description describing the business process to be supported by the computerized system should be covered.

The URS shall be generated per TEMP-129, *User Requirements Specification*.

8.2.2.2 Validation Plan (VP)

The VP is required for projects implementing new GxP Computerized Systems and for larger changes to existing GxP computerized systems. For changes to an existing computer system, the change control acts as the VP.

The VP shall focus on elements which impact GxP activities/requirements Refer to TEMP-148, Validation Plan Template.

At a high level the VP content includes:

- High level overview of the computer system and a system description including interfaces and system boundaries.
- The system architecture diagram
- Situational considerations (e.g.: Global vs. Local), hosting model, operational experience and periodic system review outcomes if applicable
- Validation approach / strategy, phases, (including the detailed lifecycle and data lifecycle, distinction between GxP and non-GxP functionality if

applicable, and relationship with other commissioning and qualification activities, justification and explanation of any variances to the basic validation approach, if relevant)

- Quality Risk Management activities including outcome of applicable risk assessments and approvals
- Roles and responsibilities
- Definition of the required CSV lifecycle deliverables
- Use of supplier resources and/or documentation (including outsourcing and use of any service models such as software as a service)
- Design review approach
- Traceability strategy
- Requirements and process for managing changes and configuration during projects: They must cover both planned and emergency updates during project phase and prior to handover to operational use. The handover point and modalities from project change management to operational change management (i.e., Change Control) must be defined as well
- Testing strategy and approach, test defect handling (if not documented in a separate Test Strategy and Plan document)
- Final acceptance and release of the system. The qualification strategy shall be based on the assessment of the risk and the complexity of the system being qualified.
- Required end user deliverables (training, SOPs, etc.). Procedures or plans required for maintaining the validated state

8.2.2.2.1 A family approach may be utilized for identical assets with identical intended use to meet the requirements of this SOP and must be defined in the VP.

8.2.2.3 Vendor / Supplier Audit Assessment

A quality assessment of vendors and service providers should be performed according to SOP-1187, *Supplier Quality Management of GxP Computerized Systems* and SOP-045, *Supplier Selection and Qualification*. The assessment may include a questionnaire or an on-site audit of the vendor depending on the complexity of the system. The results of the vendor assessment will be documented per SOP-045. A vendor quality agreement shall be established for the system per Appendix and SOP-045, as necessary. The system can be conditionally released for operational usage provided that the vendor is conditionally released per SOP-045.

Vendor documents (i.e., vendor IOQ, FAT, SAT) may be used to meet the documentation requirement stated in this procedure provided the documentation is found acceptable. Leveraging data from pre-qualification activities into qualification must be approved by the Quality unit in the system validation plan. The acceptance of the documentation can be documented in a validation plan, change control, protocol or validation summary report and approved by QA. Supplemental testing to vendor documentation is acceptable to address any requirements not completed by the vendor testing (i.e,. security requirements, audit trail, etc.).

8.2.2.4 Computer System Risk Assessment

The risk assessment identifies and documents the risks associated with the business process, and the mitigation. Identify high level system functions, functional areas, or modules that have the highest impact on patient safety, product quality, and regulated data integrity (including Electronic Records and Electronic Signatures [ERES]). The assessment shall be performed in accordance with SOP-041, *Computerized Systems Risk Assessment* and TEMP-149, *Risk Assessment Template*.

The risk assessment must be reflected in the Validation Plan (VP) and/or Test Strategy and Plan (TSP). The risk assessment must be approved by respective quality and business representatives prior to test execution.

The primary outputs of this process are the identification of required controls and the level of CSV rigor required.

8.2.2.5 System Specifications

System specifications should be developed to describe in a precise, verifiable manner the functionality and design of a system or component. System specifications may include Functional Specifications, Configuration Specifications (CS), and/or Design Specifications (DS). Depending upon the user requirements and the complexity of the system, all of these documents may not be required, or they may be combined. Specifications should be used to fulfill user requirements and be traceable to the requirements. System Specifications may be generated per TEMP-146, *System Specification Template* for GAMP5 Category 3, 4 and 5 systems. As applicable, the FS, CS, and DS can be generated as a standalone document per Appendix A.

- Functional Specification (FS) – The FS shall describe how the system will function by identifying the functions and features to be provided by the system to meet the user needs as described in the URS. The FS defines the functions and features that are to be implemented. Where available, system functionality must be implemented to reduce risks identified by the Risk Assessment.
- Configuration Specification (CS) – The CS describes how the system will be configured to meet AveXis intended use. The CS defines user roles and

permissions, configuration parameters, settings and supporting configuration files/scripts.

- Design Specification (DS) – The Design Specification including Hardware Design Specifications and Software Design Specifications (HDS and SDS respectively) and CS will specify the minimum requirements for system hardware and software, ancillary software tools, and the baseline configuration. In addition, the design specification shall include any custom code and configuration for the system or system components as applicable.
- Specifications provided by the supplier specifically for AveXis are reviewed and approved by AveXis. The approved specification must be maintained throughout the lifecycle of the system.
- Specifications must be approved prior to test script / test protocol approval.

8.2.2.6 Design Qualification / Design Review

Design reviews evaluate deliverables against standards and requirements, identify issues, and propose required corrective actions. Design reviews aim to identify and eliminate issues that would otherwise lead to changes at a later stage and are therefore to be performed before accepting the final build. The approval of the URS, Risk Assessment, and applicable specifications confirms that the proposed detailed design documentations meet the requirements established in the User Requirements Specification. Acceptance of the Design Qualification is signified by the approval of the documentation described above and concludes the design review. As applicable, perform design review per SOP-034, *Engineering Design Reviews.*

8.2.2.7 Code Review

Custom code supporting GxP functionality written by or for AveXis must be subject to a documented review. Code reviews are conducted by at least one independent person with sufficient knowledge and expertise, along with the author of the code. The extent of such reviews must be based upon risk to patient safety, product quality, and data integrity. The review must take place before formal testing starts.

The code review ensures that the quality and the structure of the code follow the established coding standards. Supplier coding activities may follow supplier procedures, provided they are evaluated and found to meet AveXis standards.

8.2.3 Infrastructure Qualification

The compliant and validated status of GxP applications are dependent upon underlying infrastructure that is in a demonstrable state of control. Components that support GxP applications must be verified and/or qualified. This may be combined with installation verification or application validation.

Infrastructure components must be installed according to manufacturer specifications and recommendations. Documentation of such installation is required, and may consist of:

- An installation verification or Installation Qualification record specifically created for the component and its required configuration settings. An Operational Qualification may be necessary to test functional requirements
- Supplier records of installation executed by supplier personnel
- A log file indicating successful installation
- A combination of the above

When supported by a documented risk assessment, it is acceptable to verify that lower risk infrastructure elements are correctly installed as part of overall system commissioning activities. In the absence of the risk assessment, full installation qualification must be completed.

For automated infrastructure build or configuration processes that automatically detect failure, a strategy of review by exception is acceptable. Absence of error messages provides adequate evidence of successful completion. Such processes must be qualified.

Infrastructure includes datacenter facilities, computer network components, servers, operating systems, layered software (e.g.: middleware, database managers, and desktop packages), peripherals, personal computers, mobile computing,

8.2.4 Computer System Installation

GxP applications shall be installed on qualified infrastructure according to the specifications. The installation process varies depending upon the GAMP software category, system architecture, and complexity. Three instances of each computer system can be implemented (Development, Test, and Production), as applicable. The development (DEV) environment is used to develop new changes without impacting the production system. The Test (TST) environment is used to formally test changes including new applications via this procedure) without impacting the production (PROD) environment. Therefore, it should mirror the production environment as close of possible.

8.2.5 Implementation and Testing Phase

During this phase, the system features and functions should be configured, enabled, tested and verified. Operation and maintenance procedures of the system should be written. The system should be installed in accordance to vendor’s installation instructions. The computer system must be tested to confirm the specifications (as per URS, and FS, CS, DS where applicable) have been met for both functionality and process Testing should be performed on several levels during development,

implementation and acceptance. The necessary extent of testing can vary greatly depending on the results of risk assessment and system category. The documents to be developed and activities to be completed are described below.

Whenever possible, testing must be performed in a separate test environment. However, if testing must be conducted in the production environment, the risk must be justified and documented, and possible precautions must be taken to protect production data. For example, test records must be clearly distinguishable from production records, and test records must be archive or segregated prior to operational use of the computerized system.

Where the computer system architecture includes segregated environments (DEV, TST, and PROD) to minimize risk and downtime, UATs are executed in either the TST or PROD environments provided they are equivalent and do not impact the outcome; where they are not, UAT is executed in the PROD environment.

8.2.5.1 Pre-Qualification

As applicable, pre-qualification activities may be performed including, but not limited to: Factory Acceptance Testing (FAT), Site Acceptance Testing (SAT) and commissioning. Pre-Qualification activities to be used will be described in the Validation Plan or test strategy plans governed by applicable change procedures. As applicable, for additional information reference SOP-035, *Commissioning and Qualification.*

8.2.5.2 Installation Qualification (IQ)

IQ is performed to verify computerized system hardware and software are properly installed and configured per vendor's and AveXis specifications. The IQ should provide a description of the computerized system including system components, the manufacturer, model, serial number, hardware/software version, and locations.

Results of the Installation Qualification are summarized in an IQ Summary Report.

8.2.5.3 Operation Qualification (OQ)

OQ testing provides documented verification that the system operates in accordance with the computerized system specifications throughout the specified operating ranges as described in the URS, FS, and CS, if applicable and/or vendor's specification.

The OQ may cover the System Test and Design Test to commensurate with the complexity of the system as defined in the System Specification document. System Test is defined to test the functionality specified in the Functional Specification document. Design Test is defined to test the custom configuration settings as specified in the Design Specification or Configuration Specification. An Operation Qualification Protocol and associated test scripts will be used to document the testing activities including any customization of the system.

Results of the Operation Qualification are summarized in an OQ Summary Report.

8.2.5.4 Performance Qualification (PQ) / User Acceptance Testing (UAT)

PQ testing provides documented verification that a computerized system performs its intended functions in the production environment under business process conditions and in accordance with User Requirement Specifications and/or approved Standard Operating Procedures. The PQ may cover the Configuration Test and/or the End-to-End business process testing and/or system suitability test. A Performance Qualification Protocol and associated test scripts will be used to document the testing activities.

PQ and User Acceptance Testing terminology can be used interchangeably.

Results of the PQ are summarized in a PQ Summary Report.

It is permissible to execute different phases of testing (i.e. OQ Functional Testing and UAT) in parallel. This is done “at risk” which means that if an issue is identified during a later phase of testing, it may require previously executed successful testing to be re-executed following the discrepancy.

8.2.5.5 Discrepancies (Exceptions)

A discrepancy is a departure from an approved qualification test specification during execution, e.g.: results which fail to meet the pre-defined acceptance criteria.

Discrepancies should be fully investigated and justified. Test discrepancies generating during IQ, OQ, PQ/UAT should be addressed and resolved. Discrepancies shall be documented following guidance per SOP-632, *Validation Exception Record*.

Discrepancies for qualification should be summarized in the qualification report.

8.2.5.6 Protocol Summary Report

Upon completion of the IQ/OQ/PQ, a protocol summary report maybe approved to summarize the results of the IQ/OQ/PQ and can be combined (i.e.IQ/OQ/PQ Summary Report or conclusions embedded within the test protocol) using TEMP-151, *Protocol Report Template*.

The summary report provides:

- An overview of the test execution
- An overview of all closed and open test discrepancies
- A clear statement of the success or failure of the testing
- Project change request and status, if applicable

The Protocol Summary Report(s) and Validation Summary Report may be combined into one document-Validation Summary Report. The Validation Plan must detail the

approach and release of systems or modules by use of Protocol Summary Reports and Validation Summary Reports.

8.2.5.7 Traceability Matrix

A Traceability Matrix should trace the user requirements, system design, and testing through to the documentation where the requirements are verified. The Traceability Matrix can be a standalone or embedded within the Validation Summary Report. Refer to *TEMP-147, Traceability Matrix Template,* for the generation of the Traceability Matrix.

8.2.5.8 Validation Summary Report

A Validation Summary Report should summarize the conclusion regarding the suitability of the system for its intended use, summarize activities specified by the VP, summarize test summary reports if applicable, summarize discrepancies, and list all deliverables generated during the process. If any activities are left open that will carry past system release include justification for acceptance and reference associated CAPA(s).

8.2.5.9 General Considerations

Depending upon the nature of the system, qualification test protocols may be combined into one document. All system requirements and specifications should be traceable to and verified by testing occurring during the qualification and/or design qualification process.

Test plans and acceptance criteria should be described in the respective protocols IQ, OQ, PQ/UAT. Guidance following template TEMP-145, *Protocol Template for Installation / Operational / Performance Qualification (Systems).*

Chronology of IQ, OQ, and PQ activities completion should be enforced.

Test discrepancies generated during IQ, OQ, PQ/UAT should be addressed and resolved before proceeding to subsequent activities (i.e., test discrepancies generated during IQ activities should be resolved before proceeding to OQ activities).

Approval of the Protocol Report or Validation Summary Report releases the system for Production use in accordance with validation plan documentation (e.g., VP, Change Control Validation Impact Assessment).

8.2.6 Operation and Maintenance Phase

This phase describes the process during operation and maintenance of a computerized system after the system is validated for intended use. Operations manuals (i.e., user manual/system manual) and procedures must be available and followed to maintain the system in a validated state. The elements of this phase are described below.

8.2.6.1 Training

All users should be trained before operating the system and documented training should be available.

Training requirements (i.e. SOP, Manual, etc.) procedure to provide information on how to obtain access to the system and what trainings are needed must be defined.

8.2.6.2 Security / System Access Management

Access Rights are to be established to ensure that only persons with appropriate training and authorizations have access to the system and should follow the Authorization Role Concept. The Authorization Role Concept defines what kind of authorization/permissions are assigned to each system role and to what business organization ensuring segregation of roles are enforced. An Access Form should be available to document creation, modification, or removal of access rights.

8.2.6.3 Periodic Review of Access

A Periodic Review of access rights must be performed by System Owner and/or SME. The frequency and scope of the review can be defined based on risk.

8.2.6.4 Security Monitoring

Security Monitoring should be performed by System Owner and/or SME. The frequency and scope of the security monitoring can be defined based on risk.

8.2.6.5 Incident Management

An incident management process should be established to manage unexpected behavior (incidents) reported for a system. Incidents are to be corrected and investigated for root cause so controls can be established to prevent recurrence. Incidents that are considered to affect cGxP status should be raised to a Non-Conformance. Refer to SOP-005, *Non-Conformance and CAPA System*.

8.2.6.6 Patch and Update Management

A process shall be available to define how patch updates are to be applied for the system and the documentation for patch management.

8.2.6.7 Audit Trail

Audit trail is defined as a secure, computer-generated, time-stamped electronic record that allows for reconstruction of events relating to the creation, modification, or deletion of an electronic record.

Processes should be available to describe how and when to operate an audit trail for the system.

Determination of scope and audit trail review frequency should be based on risk to product quality and patient safety.

Processes should be defined for performing periodic review of system audit trail and routine audit trail review.

- System Audit Trail Review is comprised of reviewing changes to critical system configuration, roles/privileges settings, time/date settings and deleted actions.
- Routine audit trail review should be performed on data that is captured during routine operations of the system and can be performed as part of the review of the critical GxP data (review for changes to critical data). Usually this is performed as part of the routine data review/approval process.

8.2.6.8 Data Management and Data Review

Data should be attributable to the person generating the data, legible and permanent, contemporaneous, original (or true copy) and accurate complying with the ALCOA principles.

Processes should be available to describe the raw data for the system.

Processes should be available to describe the data review process for reported data against raw data and all processed data.

Data deletion is not allowed and shall be prevented by established controls unless a data archiving activity is required to take data off the system.

8.2.6.9 Change Management Process

System level changes including hardware, software, configuration, master data changes, repairs (replacement of components) relevant to the system should follow the change control procedure. The change should assess the need for testing/regression testing to ensure that existing functionality is not negatively impacted by the change. Based on risk, an abbreviated set of documents can be completed to verify the change. See SOP-004 for details.

8.2.6.10 System Periodic Review

Periodic review of the system shall be performed to ensure a system continues to maintain its validated state, preserving the integrity of the system and its data throughout the complete lifecycle of the system.

A Periodic Review report will be generated to document the results of the system periodic review. Periodic review frequency will be based on system category and impact. Guidance per SOP-418, Periodic Review of Computerized Systems, should be followed.

8.2.6.11 Backup and Restore

Processes that provide electronic records backup and restore functions have to be established and documented. Backup operations encompass all relevant data,

including raw data and metadata, and must be automated wherever possible; however, procedural records backup operations must be formally implemented where an automated process is not available.

Backup procedures must include:

- Backup plan elements, such as scope, schedules
- Mechanism for verifying backups are complete and correct (and ensuring data integrity and accuracy)
- Process for reviewing backups operations and an escalation process for failed backup operations
- Backup media management
- Process for restoring records

The backup and restore processes are tested during the initial validation and monitored periodically.

8.2.6.12 System Administration

System Administration is the routine support of systems to ensure that they are reliable and function optimally during operations. System Administration activities will follow their respective internal procedures and should be described in the specific procedure. When System Administration is done internally at the site, then the respective processes and requirements are described in the specific procedure.

8.2.6.13 Data Archiving and Retrieval

Data stored in the system must be readable and retrievable throughout the associated record retention period. See POL-006 and SOP-362 for record retention requirements. In case of moving records out of the production system and storing them in a separate environment (off-line Archiving), they should be protected against further changes.

The archival process includes:

- Procedures for retrieving records that have been archived
- Procedures for ensuring archival operations are successful
- Establishment of media exercise requirements where applicable
- Definition of the record retention schedule and the process for records destruction

8.2.6.14 Data Migration

If a system is being implemented to replace another data management system, whether the data will be migrated to the new system or archived should be

determined and documented. In any situation, if the data is to be migrated, the migration process should be documented in a Data Migration Plan or Validation Plan. The importance and sensitivity of the data, and the technical risk of the transformation define the extent of the migration verification. Based on harm of data lost the verification strategy may need a statistical method of sampling., . A Data Migration Summary Report or Validation Summary Report should include a summary of the activities and their results, statements about acceptance and a statement about the general validation status of the system.

Data migration planning has to be conducted when:

- Transferring an application or its data to a new database platform
- Converting data as part of the computerized system upgrade (software or hardware)
- Re-hosting the functionality of an existing computerized system to an entirely new computerized system

8.2.6.15 Document Management

System documentation is kept up to date throughout the system life cycle and should be securely stored according to procedures. Electronic records for the system should be retrievable throughout the defined retention period per POL-006 and protective measures should prevent the use of unapproved or obsolete documentation (e.g., version control).

8.2.6.16 Disaster Recovery

Disaster recovery strategy that describes the process for recovering the system after hardware and software failures, power failure, natural disasters, security breaches, etc. should be defined. The System Owner is responsible to ensure that where IT owns the Disaster recovery activities, a defined process specifically for such failures is described.

8.2.7 Decommissioning / Retirement Phase

During the Decommissioning / Retirement Phase, the computerized system is formally discontinued from operational use, marking the end of the system life cycle. When a computerized system is retired / decommissioned, a Retirement / Decommissioning Plan and Retirement / Decommissioning Report must be developed and approved to assure that all required regulatory information and data maintained by the system can be retrieved during the retention period required by the applicable regulations. The plan shall include the retirement/decommissioning strategy considering roles and responsibilities, system, data, documentation and impact to other interface systems.

APPENDIX A: DELIVERABLES AND RESPONSIBILITY'S MATRIX

Note: Roles can be combined, and must be documented on the approval section of the document

CSV	Business Approver	Technical Approver	Quality Approver	GxP Classification	Comment
Computer System Classification					
Computer System Classification	BSO	TSO	QA / QA eCPL	Low	Classification documents for all CS, including Non-GxP must be approved by QA / QA eCPL
	BSO	TSO	QA / QA eCPL	Medium	
	BSO	TSO	QA / QA eCPL	High	
Supplier Quality Assessment					
Supplier Quality Check List (SQCL)	N/A	N/A	N/A	Low	N/A (SQCL is not required for Low GxP classified systems)
	N/A	N/A	QA / QA eCPL	Medium	
	N/A	N/A	QA / QA eCPL	High	
Quality Assurance Agreement					
QAA	N/A	N/A	N/A	Low	N/A (QAA is not required for Low GxP classified systems)
	N/A	N/A	QA / QA eCPL	Medium	
	N/A	N/A	QA / QA eCPL	High	
Validation Deliverables					
Validation Plan	BSO	TSO	QA / QA eCPL	Low	
	BSO	TSO	QA / QA eCPL	Medium	
	BSO	TSO	QA / QA eCPL	High	
User Requirement Specification	BSO or delegate	TSO or delegate	Validation / QM	Low	
	BSO	TSO	Validation / QM	Medium	
	BSO	TSO	QA / QA eCPL	High	
Data Integrity Assessment	BSO or delegate	TSO or delegate	Validation / QM	Low	
	BSO	TSO	Validation / QM	Medium	
	BSO	TSO	QA / QA eCPL	High	
Functional Specification	BSO or delegate	TSO or delegate	N/A	Low	
	BSO	TSO	N/A	Medium	
	BSO	TSO	N/A	High	

CSV	Business Approver	Technical Approver	Quality Approver	GxP Classification	Comment
Configuration Specification / Design Specification*	N/A	TSO or delegate	N/A	Low	CS/DS are required based on the technology classification. For simples application content can be combined with FS
	N/A	TSO or delegate	N/A	Medium	
	N/A	TSO or delegate	N/A	High	
Code Review*	N/A	SME	N/A	Low	Code Review is required based on the technology classification. Review approval must be performed by peer
	N/A	SME	N/A	Medium	
	N/A	SME	N/A	High	
Data Conversion / Migration Plan (DC/MP)*	SME	TSO	BPO or BSO	Low	Where available and defined, Data Owner shall cover the Business approver role.
	BSO or BPO	TSO	Validation / QM	Medium	
	BSO or BPO	TSO	QA / QA eCPL	High	
Functional Risk Assessment (FRA)	SME	TSO	BPO or BSO	Low	
	BSO / BPO	TSO	Validation / QM	Medium	
	BSO / BPO	TSO	QA / QA eCPL	High	
Test Strategy Plan (TSP)*	N/A	N/A	N/A	Low	N/A (TSP is not required for Low GxP classified systems)
	BSO	TSO	Validation / QM	Medium	
	BSO	TSO	QA / QA eCPL	High	
Traceability Matrix (TRM)	N/A	N/A	N/A	Low	No formal approval required on information about traceability
	N/A	N/A	N/A	Medium	
	N/A	N/A	N/A	High	
IQ	N/A	SME	TSO	Low	Records created from the execution of the specification have to be approved by the same functions
	N/A	TSO	Validation / QM	Medium	
	N/A	TSO	Validation / QM	High	
OQ	N/A	SME	TSO	Low	Records created from the execution of the specification have to be approved by the same functions
	N/A	TSO	Validation / QM	Medium	
	N/a	TSO	Validation/ QM	High	
PQ	SME	N/A	Validation/ QM	Low	Records created from the execution of the specification have to be approved by the same functions
	BPO or BSO	N/A	Validation/ QM	Medium	
	BPO or BSO	N/A	Validation/ QM	High	
Data Conversion / Migration Report (DCMR)*	SME	TSO	BPO or BSO	Low	Where available and defined, Data Owner shall cover the Business approver role
	BPO or BSO	TSO	Validation/ QM	Medium	
	BPO or BSO	TSO	QA / QA eCPL	High	
	N/A	N/A	N/A	Low	

CSV	Business Approver	Technical Approver	Quality Approver	GxP Classification	Comment
Test Summary Report (TSR)*	BSO	TSO	Validation/ QM	Medium	Where available and defined, Data Owner shall cover the Business approval role
	BSO	TSO	QA / QA eCPL	High	
Validation Report (VR)	BSO	TSO	QA / QA eCPL	Low	
	BSO	TSO	QA / QA eCPL	Medium	
	BSO	TSO	QA / QA eCPL	High	
Operational Mgmt Processes	BSO	TSO	Validation/ QM	Low	
	BSO	TSO	QA / QA eCPL	Medium	
	BSO	TSO	QA / QA eCPL	High	
Archival Plan (AP) / Retirement Plan (RP)	BSO	TSO	Validation/ QM	Low	
	BSO	TSO	QA / QA eCPL	Medium	
	BSO	TSO	QA / QA eCPL	High	
Archival Report (AR) / Retirement Report (RR)	BSO	TSO	Validation/ QM	Low	
	BSO	TSO	QA / QA eCPL	Medium	
	BSO	TSO	QA / QA eCPL	High	
System Operation					
Incident Management (IM) / Problem Management (PrM)	BPO or delegate	AM	Validation/ QM	Low	
	BPO	TSO	QA / QA eCPL	Medium	
	BPO	TSO	QA / QA eCPL	High	
Disaster Recovery Plan (DRP)	SME	TSO	BPO or BSO	Low	
	BPO or BSO	TSO	Validation/ QM	Medium	
	BPO or BSO	TSO	QA / QA eCPL	High	
Disaster Recovery Report (DRR)	SME	TSO	BPO or BSO	Low	
	BPO or BSO	TSO	Validation/ QM	Medium	
	BPO or BSO	TSO	QA / QA eCPL	High	
Business Continuity Plan (BCP)	SME	TSO	BPO or BSO	Low	
	BPO or BSO	TSO	Validation/ QM	Medium	
	BPO or BSO	TSO	QA / QA eCPL	High	
Periodic Review Report (PRR	BSO	TSO	QA / QA eCPL	Low	
	BSO	TSO	QA / QA eCPL	Medium	
	BSO	TSO	QA / QA eCPL	High	

* Conditional Deliverables

DOCUMENT HISTORY

SOP No.	Version No.	Description of Change
SOP-279	1.0	New SOP
SOP-279	2.0	Section 3: Added responsibility for generating change control to system owner. Moved responsibility to manage access rights, collects, and tracks system defects, and maintain validated state to IT. Removed the responsibility to author documentation from system owner. Removed the responsibility to support in the implementation (development, configuration, installation) from the technical SME. Section 6: Added two Forms, nine Policies, seven SOPs, and seven Templates. Removed references to 21 CFR Part 58. Section 8.2.3 Added a section on protocol report. Changed 'Summary Report' to 'Validation Plan Summary Report'. Added a statement 'Approval of the Protocol Report or Validation Plan Summary Report releases the system for Production use'. Section 8.2.4 Updated Data Archiving and Retrieval. Updated font and font size throughout document for consistency.
SOP-279	3.0	Include 2013/C 343/01 EU Guidelines on Good Distribution Practice of Medicinal Products for Human Use in references and scope. Updated references to AveXis Inc. to AveXis. Include Responsible Person role in Section 3.
SOP-279	4.0	Updated overall SOP format; removed tables and used paragraph formatting. Sequential section numbering assigned. Removed Table of Contents. Section 2: Removed exclusion of IT infrastructure as out of scope. Added IT, Automation systems, and IT Infrastructure to the scope. Section 3: Renamed and Added roles and responsibilities. Added Business Process Owner, System Infrastructure provider, System Supplier, and Administrator. Updated "System User" to "System User Groups". Section 6: Added / removed references to documents and only included documents within the SOP. Section 8: Added subsections. 8.2 updated "System Life Cycle Phases" to "Validation Life Cycle Phases". 8.2.1.1 and 8.2.1.2 to outline system impact assessment and data integrity assessment; reference to FORM-302 was replaced with FORM-355 and SOP-555. General updates were made throughout for clarification. Added Section 8.2.2.2.1 to include family approach description. Added Section 8.2.2.5 to include description and explanation for FS, CS, and DS use. Added Section 8.2.2.6 Design qualification description. Added Section 8.2.3.1 Pre-Qualification for guidance. Added Section. Added Section 8.2.4.6 Patch and Update Management. Updated Section 8.2.5 Decommissioning / Retirement Phase to incorporate contents from draft SOP-427. Removed Analytical instrument Qualification Table, this information is covered in SOP-555, system Impact Assessment.
SOP-279	5.0	Δ Update SOP-279 to align with NVS SOP-7037712, STD-8037786, FRM-8037791, SOP-8027419, and SOP-7041072 per CAPA-844.Δ

SOP No.	Version No.	Description of Change
		Section 2 Clarified scope for systems to use SOP-279. Section 3 Updated the Roles and Responsibilities to align with Novartis Roles and Responsibilities. Section 6 Updated References with supporting documents, SOP-1187, SOP-1018, TEMP-323, WI-276, POL-006, and SOP-362 and within the document body. Section 7 Updated as necessary with alignment to Novartis procedures. Sections 8.2.1.1 through 8.2.1.2 was updated to align with NVS SOP-7037712, SOP-8027419, and STD-8037786 to include Δ "a computer system classification to allow a scaled qualification and validation strategy" Δ per CAPA-844. Section 8.2.2.2 was updated to Δ "add requirements for validation plans" Δ to align with NVS SOP-7037712 per CAPA-844. Section 8.2.2.3 added reference to Δ "SOP-1187" Δ to align with Novartis SOP-7041072 per CAPA-844. Section 8.2.2.4 added instructions that Δ "the Risk Assessment will determine qualification vigor and must be discussed in the Validation Plan" Δ to align with NVS SOP-7037712 and STD-8037786 per CAPA-844. Section 8.2.2.5 added instructions for functional specification Δ "Where available, system functionality must be implemented to reduce risks identified by the Risk Assessment" Δ to align with NVS STD-8037786 and SOP-8027419. Section 8.2.2.6 reworded design qualification and design review wording. Section 8.2.2.7 added Δ "Code Review requirements" Δ to align with NVS SOP-7037712. Section 8.2.3 and 8.2.4 added specific Δ "Infrastructure qualification requirements and computer system installation guidelines" Δ to align with NVS SOP-7037712 per CAPA-844. Section 8.2.5.4 added permissible risk based testing strategy to allow for execution flexibility. Section 8.2.5.6 added Δ "details deliverables for test reports and the allowance to combine the test report and final summary report" Δ to align with NVS SOP-7037712 per CAPA-844. Section 8.2.5.8 added instructions that Δ "a CAPA with justification is required if any activities are left open that will carry past system release" Δ to align with NVS-7037712 per CAPA-844. Section 8.2.6.11 added Δ "Backup and Restore process and qualification of Backup and Restore as requirements for the implementation of a system" Δ to align with NVS SOP-7037712 per CAPA-844. Sections 8.2.6.13 and 8.2.6.14 added Δ "details for Archival and Data Migration processes" Δ to align with NVS SOP-7037712 per CAPA-844. Appendix A updated the Δ "approval matrix as deliverables" Δ to align with NVS STD-8037786 per CAPA-844