TABLE OF CONTENTS

1 PURPOSE

This document describes the process for performing the IT Solution Delivery Lifecycle (SDLC) to deploy a IT supported solution in accordance with IT Policy, SOP-0022 Service and Solution Lifecycle management.

2 AUDIENCE

This procedure is intended for colleagues, contractors and vendors who participate in IT SDLC activities.

3 SCOPE

3.1 In Scope

- This procedure applies to new or modified solutions that will be deployed into IT supported or controlled environments including vendor supported environments.

- Changes to existing solutions are governed by *SOP-0839 IT Change Management*. The Change Management process is used to determine the applicable SDLC requirements for solution changes or upgrades. SDLC elements required to support a change are governed by this procedure (*SOP-0906*).

3.2 Out of Scope

- Technology that is not IT supported or not maintained in a controlled environment. Examples of these environments may include: proof of concept, proof of technology, new installation (product, server, system) for evaluation, sandbox environments and development environments.

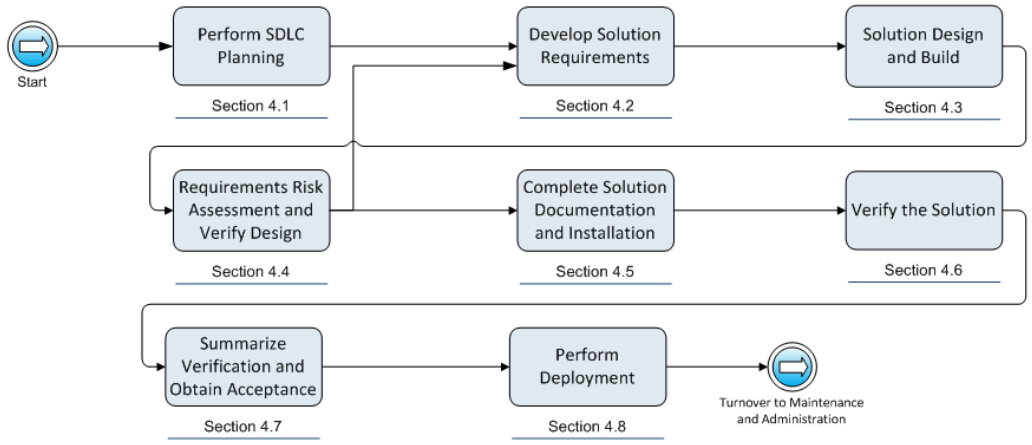
- Retirement of a solution when it is no longer needed is governed by *SOP-0908 IT SDLC Retire Phase.*

- Infrastructure Qualification is governed by *SOP-0977 IT Infrastructure Qualification*. Qualification activities may be carried out as part of solution delivery as long as the elements of both procedures are met.

4 PROCEDURE

The Solution Delivery LifeCycle ensures that IT has appropriate processes and procedures to establish and maintain solution quality. The LifeCycle approach entails defining and performing activities in a systematic way including planning, requirements gathering, design, build, and verify processes to deploy and maintain IT solutions.

Note: Underlined blue text in the document below are links to definitions in the IT Glossary.



The steps are described in a linear fashion; however, some steps may occur in a direct sequence, and some activities may be conducted in parallel or iteratively.

All solutions follow the process described above however SDLC elements and approvals are applied based on regulatory risk. Elements are the activities and deliverables that support a project. Solutions are required at minimum to have a Baseline set of elements and approval. Baseline elements are considered the minimum requirement for good software development. Solutions subject to Sarbanes Oxley (SOX) and Validation (GxP) require additional elements and approvals to satisfy external regulations e.g. USA Food and Drug Administration (FDA) Code of Federal Regulations. Regulatory risk is determined through solution profiling and is documented in the Plan (or Validation Plan) element.

Baseline Elements	SOX Elements	Validation Elements
Plan	Plan	Validation Plan
Requirements	Requirements	Requirements
Design / Installation Information (Custom / Configured)	Design Specification	Design Specification
	Installation Instructions / Verification	Installation Instructions/Verification
		Environment Acceptance
		Verification Plan
		Verification Scripts
Verification Evidence	Verification Evidence	Verification Evidence
		Verification Summary
Acceptance Statement	Traceability	Traceability
	Acceptance Statement	Acceptance Statement
		Validation Summary

In the process input and output steps below, items marked with **bold font** are elements represented in Appendix B. Process step Inputs and Outputs are defined in section 4.1 to 4.8 using a ✓ to indicate if required for Baseline, SOX or Validation.

4.1 Perform SDLC Planning

Process Step Inputs:	**Baseline**	**SOX**	**Validation**
• Initiated project or approved work	✓	✓	✓
• Vendor Assessment (Baseline & SOX based on risk)			✓

Step	**Actions**	**Roles**
4.1.1	Determine the compliance requirements applicable for the solution by completing a Solution Profile (also known as CRP) as per SOP-0012. Using the Solution Profile, determine if Baseline, SOX or Validation SDLC elements and approvals apply.	Project Team
4.1.2	Engage a Business Unit Quality Assurance (BUQA) representative for solutions that need to comply with GMP regulations.	Technical Rep
4.1.3	Document the strategy and approach for meeting the minimum required elements as defined in Appendix A in the Plan (or Validation Plan).	Technical Rep

Process Step Outputs:	**Baseline**	**SOX**	**Validation**
• Solution Profile (also known as CRP)	✓	✓	✓
• **Plan**	✓	✓	
• **Validation Plan**			✓

4.2 Develop Solution Requirements

Process Step Inputs:	**Baseline**	**SOX**	**Validation**
• High level business requirements (if applicable)	✓	✓	✓
• Solution Profile (also known as CRP);	✓	✓	✓
• **Plan**	✓	✓	
• **Validation Plan**			✓

Step	**Actions**	**Roles**
4.2.1	From the Solution Profile completed in step 4.1.1, obtain the applicable Common Requirements Set (CRS) Compliance Requirements to determine the necessary IT controls for the solution.	Technical Rep
4.2.2	Develop and document User and Solution requirements based on business need as specified in Appendix B.	Project Team
4.2.3	Identify and document other standards, controls, and specifications in addition to User and Solution requirements; such as, architecture, and technology specifications.	Technical Rep

Process Step Outputs:	**Baseline**	**SOX**	**Validation**
• **Common Requirements Set (CRS)**	✓	✓	✓
• Documented **Requirements**	✓	✓	✓

4.3 Solution Design and Build

Process Step Inputs (as applicable to solution):	Baseline	SOX	Validation
• Documented **Requirements**	✓	✓	✓
• **Plan**	✓	✓	
• **Validation Plan**			✓
• Known solution hardware and software components	✓	✓	✓

Step	Actions	Roles
4.3.1	Custom– Functionality customized to meet user/solution requirements**.** For custom functionality, determine if coding standards are required for the solution per the Plan (or Validation Plan). If coding standards are required, identify existing or develop solution Coding Standards to govern good coding practices and as an input to the Code Review. Begin to document the solution design per Appendix B.	Technical Rep
4.3.2	Configured – Functionality configured to meet user/solution requirements**.** Draft the Configuration Specification component (if applicable) of the design per Appendix B.	Technical Rep
4.3.3	Technical Architecture **-** Structure of a solution or IT service. Determine if any new or revised Technical Architecture is required for the solution. If new or revised architecture is required, draft or update the Technical Architecture component of the design per Appendix B.	Technical Rep
4.3.4	Draft or reference Installation Instructions/Information to govern the reproducible installation of the verification environment as per the Plan (or Validation Plan). See Appendix B for Installation Instructions components.	Technical Rep
4.3.5	Refine requirements and/or solution based on preliminary verification of solution functionality. Examples of preliminary verification could include dry run or iterative testing.	Project Team
4.3.6	Confirm that all requirements are addressed through the design, including all requirements obtained from the Common Requirements Set (CRS).	Project Team
4.3.7	For an iterative development process, repeat steps 4.3.5 and 4.3.6 with inclusive team design review sessions until all solution functionality satisfies business needs.	Project Team

Process Step Outputs (as applicable to solution):	Baseline	SOX	Validation
• **Design and Installation Information**	✓		
• Coding Standards; Draft **Design Specification**, including configuration and technical architecture components		✓	✓
• Draft or referenced **Installation Instructions**		✓	✓
• Final **Requirements**	✓	✓	✓
• Developed solution	✓	✓	✓

4.4 Requirements Risk Assessment & Verify Design

Process Step Inputs:	Baseline	SOX	Validation
• Final **Requirements**	✓	✓	✓

Step	Actions	Roles
4.4.1	Perform the Requirements Risk Assessment to determine the appropriate level of testing as per Appendix C. This risk rating determines the type of testing required for all requirements Use risk influencers as appropriate and as documented in the plan (or Validation Plan).	Project Team
4.4.2	Perform and document a Design Verification per Appendix B	Project Team

Process Step Outputs:	Baseline	SOX	Validation
• Requirements Risk Assessment results	✓	✓	✓
• Design Verification			✓

4.5 Complete Solution Documentation and Installation

Process Step Inputs (as applicable to solution):	Baseline	SOX	Validation
• **Plan**	✓	✓	
• **Validation Plan**			✓
• Final **Requirements**	✓	✓	✓
• **Design and Installation Information**	✓		
• Coding Standards; Draft **Design Specification**, including configuration and technical architecture components		✓	✓
• Draft or referenced **Installation Instructions**		✓	✓

Step	Actions	Roles
4.5.1	**Custom Functionality** Execute the following steps if the solution includes custom development and as required by the Plan (or Validation Plan): • Ensure Coding Standards are final prior to Code Review. • Perform Code Reviews against the Coding Standards per Appendix B. Document the Code Reviews. Code reviews should include technical subject matter experts and the coding team member. *The review of the code cannot be completed solely by the coding team member*. • Finalize Design Specification per Appendix B.	Technical Rep
4.5.2	**Configured Functionality** Finalize the Configuration Specification component per Appendix B if the solution includes configuration and as required per the Plan (or Validation Plan).	Technical Rep

4.5.3	**Technical Architecture** Finalize the Technical Architecture documentation per Appendix B if the solution includes new or modified Technical Architecture component and as required per the Plan (or Validation Plan).	Technical Rep
4.5.4	Finalize Installation Instructions or confirm the referenced Installation Instructions as required per the Plan (or Validation Plan).	Technical Rep
4.5.5	Install and document the software component of the solution according to the Installation Instructions for controlled environments (test, production, etc.) and as required per the Plan (or Validation Plan). Verify the install (SOX and Validation only) If an exception occurs, record and disposition per the solution's Verification Exception/Deviation Management process.	Technical Rep
4.5.6	Verify and document that the configuration is complete and correct according to the Configuration Specification documentation if the solution requires configuration. If an exception or deviation occurs, follow the solution's Verification Exception/Deviation Management process.	Technical Rep
4.5.7	Document the Environment Acceptance for solution functional verification per Appendix B (Validation only).	Technical Rep

Process Step Outputs (as applicable to solution):	**Baseline**	**SOX**	**Validation**
• **Design and Installation Information**	✓		
• Coding Standards or Reference; Code Review		✓	✓
• **Design Specification**, including configuration and technical architecture components		✓	✓
• **Installation Instructions/Verification** or Reference		✓	✓
• Executed Installation Instructions		✓	✓
• Executed Configuration Specification		✓	✓
• Documented **Environment Acceptance**			✓

4.6 Verify (test) Solution

Process Step Inputs:	Baseline	SOX	Validation
• **Requirements** and Requirements Risk Assessment results	✓	✓	✓
• **Plan**	✓	✓	
• **Validation Plan**			✓
• Verification Exception/Deviation Management process		✓	✓

Step	Actions	Roles
4.6.1	Determine the verification (testing) approach to ensure requirements are met for the solution considering: • Requirements Risk Assessment outcome • Verification strategy (Appendix C) Document the Verification Plan and executable documents (for example Verification Scripts). The Verification Plan, Verification Scripts and Requirements must be approved prior to beginning formal verification activities (SOX and Validation only).	Project Team
4.6.2	Confirm verification is traceable to requirements and design elements and other applicable controls and specifications per Appendix B. Document the traceability (SOX and Validation only).	Project Team
4.6.3	Execute the Verification Plan per Appendix B and Appendix C and in accordance with good documentation practices as described in *SOP-0001 IT Records Management*. If an exception occurs, record and disposition per the solution's Verification Exception/Deviation Management process.	Project Team
4.6.4	Review the results for the verification activities conducted and the documentation produced.	Project Team

Process Step Outputs:	Baseline	SOX	Validation
• **Verification Scripts**			✓
• **Verification Evidence**	✓	✓	✓
• **Traceability** of verification to requirements and design		✓	✓
• Dispositioned verification exceptions and deviations	✓	✓	✓

4.7 Summarize Verification and Obtain Acceptance (for Release)

Process Step Inputs:	Baseline	SOX	Validation
• **Verification evidence**	✓	✓	✓
• Traceability of verification to requirements and design		✓	✓
• Dispositioned verification exceptions and deviations	✓	✓	✓

Step	Actions	Roles
4.7.1	Document the verification (test) execution in the Verification Summary as per Appendix B, and ensure that all exceptions and deviations are investigated and dispositioned following the solutions Verification	Project Team

	Exception and Deviation Management process prior to approving the Verification Summary (Validation only).	
4.7.2	Collaborate with customer and stakeholders to ensure acceptance criteria, as documented in the Plan, was satisfied. Document the Acceptance Statement as per Appendix B.	Technical Rep
4.7.3	For solutions that are to be released for production use and do not require additional deployment activities, document the Validation Summary as per section 4.8.3 below. Note: the Acceptance statement and Validation Summary can be combined. (Validation only).	Project Team
4.7.4	Update the CRS disposition per the CRS Assessment in IPRM as required. (Refer to the SOP-0012, Compliance Risk Profiles).	Technical Rep
4.7.5	Review key Configuration Management Database (CMDB) solution information to ensure it is current and correct in accordance with SOP-0897, IT Configuration Management.	Technical Rep

Process Step Outputs:	**Baseline**	**SOX**	**Validation**
• **Verification Summary**			✓
• **Acceptance Statement**	✓	✓	✓

4.8 Perform Deployment

Process Step Inputs:	**Baseline**	**SOX**	**Validation**
• Deployment activities defined in the **Plan or Validation Plan** (Section 4.1: Perform SDLC Planning)	✓	✓	✓

Step	**Actions**	**Roles**
4.8.1	Engage the appropriate quality authority. For GMP solutions, the Quality Authority at each site/region approves local validation documentation and is responsible for ensuring that the local implementation of GMP core systems is addressed.	Technical Rep
4.8.2	Execute and document Deployment as per the Plan or Validation Plan, e.g., deployment can be documented in the appropriate change record or Validation Summary (Appendix B).	Project Team
4.8.3	Document the Validation Summary as per Appendix B. Corrective actions taken or corrective action plans must be reviewed and approved prior to, or concurrent with, approval of the Validation Summary. Update the GMP computerized inventory as applicable when the solution is validated (Validation only).	Project Team

Process Step Outputs:	**Baseline**	**SOX**	**Validation**
• Executed Deployment and Documented Deployment results	✓	✓	✓
• **Validation Summary**			✓

5 ROLES AND RESPONSIBILITIES

Role	Responsibility
Project Team	• Collaboration between the functional roles, Business Unit, Technical Unit, BTQA and BUQA (depending on the need of the solution). • Execute SDLC activities such as develop and refine requirements, assess solution and requirement risk, design, build and verify. • Identify when it is appropriate to seek input from other quality organizations, Global Risk Compliance and Control group (GRCC), or other corporate compliance organizations, such as the Global Privacy Office.
IT Quality Assurance (BTQA)	• The IT Quality Assurance Representative is responsible to assure the SDLC methodology is followed and that the solution's deliverables are compliant and consistent with SOPs and applicable CRS requirements for solutions subject to SOX and Validation regulations only.
Business Representative	• The Business Representative is ultimately responsible for ensuring that the solution and its operation is in compliance and fit for its intended use in accordance with all applicable SOPs and regulatory requirements throughout it useful life.
Business Unit Quality Assurance (BUQA)	The Business Unit Quality Assurance represents Global Quality Operations (GQO) and serves as the Quality Authority for GMP Solutions. Responsibilities include: • Ensuring solutions comply with computer system regulations • Coordinating with the appropriate quality SME group to ensure correct quality representation for business areas where Quality Systems &Compliance(QS&C)-Validation is not the quality authority • Ensure risk/criticality assessments consider the impact of related computer system regulations affecting the validation of the system For GMP solutions, the Quality Authority at each site/region approves local validation documentation and is responsible for ensuring that the local implementation of GMP core systems is addressed
Technical Representative	• The IT Representative is ultimately responsible for design, development, testing (including planning and scheduling of validation as applicable) and deployment of the solution, for availability, support and maintenance of the solution in accordance with all applicable SOPs. The IT representative is also responsible for design, development and testing of security controls. • For Baseline solutions, the Technical Representative responsibilities also include those defined in the BTQA role.

6 DEFINITIONS

Refer to the Information Technology (IT) Glossary for definitions of terms used in this procedure.

7 RECORD RETENTION AND MANAGEMENT

The following company records may be created as a result of executing this procedure. Please refer to the following table for the retention classification of these records, per Corporate Policy (CP) 405, Records and Information Management Policy. The Enterprise Records Retention Schedule (ERRS) lists and describes Company Records according to their business purpose, function and storage requirements together with instructions for how long they should be maintained. The retention times are based upon regulatory, legal and tax requirements. See erim.pfizer.com for more information including Retention Classifications detailed below.

Record Name	Retention Classification
Plan or Validation Plan	INF 01 05
Requirements	INF 01 05
Design Documentation	INF 01 05
Installation Instructions / Verification	INF 01 05
Environment Acceptance	INF 01 05
Verification Plan	INF 01 05
Verification Evidence	INF 01 05
Verification Summary	INF 01 05
Traceability	INF 01 05
Acceptance Statement	INF 01 05
Validation Summary	INF 01 05

8 SUPPORTING REFERENCES

Record Number	Reference Title
CP 405	Records and Information Management Policy
CP 904	Software Medical Device Corporate Policy and Procedure
SOP-0022	Service and Solution Lifecycle Management
SOP-0001	IT Records Management
SOP-0012	Compliance Risk Profiles
SOP-0839	IT Change Management
SOP-0849	Vendor Compliance Assessment Services
SOP-0887	IT Personnel Qualification
WTSO-0897	IT Configuration Management
SOP-0933	Periodic Review
SOP-0959	IT Asset Lifecycle Management
SOP-0977	IT Infrastructure Qualification

9 REVISION HISTORY

Version	Author	Date	Revisions
3.0	William Dougherty;	29 June 2015	• Combined SOP-0905 and SOP-0907 into this document and renamed SOP-0906.

Version	Author	Date	Revisions
	Allison Volpe		• Revised procedure to identify the requirements for Baseline, SOX, and GXP systems. • Minor updates to document for clarification • Added content from SOP-0905 and • Added content from SOP-0907 • Section 1 and 3 – Minor updates and re-organization with Purpose and Scope sections. • Section 3.2 – Updated to list Retirement as Out of Scope. • Sections 4.1 through 4.8 – Updated for consistency, and to more clearly identify items that only apply to SOX or GXP systems. Clarified process steps requirements. • Section 5 – Update roles and responsibilities • Section 6 – Removed definitions that are already covered as part of the IT Approved Terms glossary • Appendix A – Elements Matrix updated to identify required elements for Baseline, SOX, and GXP systems. • Appendix B – Element component list updated to align with updated Elements from Appendix A, and to clearly identify the Elements or components that only apply to SOX or GXP systems. Added data migration component to Plan and Validation Plan. • Appendix C – Updated Verification strategy to focus on the requirement risk assessment and provide testing clarity.
2.0	Lisa M. Krepel	05-AUG-2013	Minor updates to align with Change Management and Infrastructure Qualification: • Updated scope, definitions and roles • Updated process flow to follow current standards. • Reformatted to follow current SOP template.
1.0	Martha Holland	17 APR 2012	Minor formatting and grammar corrections, including change of version number above in this table from 1.0 to 0.1. (Note: 0.2 was made to 1.0 to clarify version history)
0.1	Richard Riotto	20-DEC-2011	First Issue.

10 APPENDICES

Appendix	Appendix Name
A	Elements Matrix
B	Element Components
C	Verification Strategy

APPENDIX A ELEMENTS MATRIX

The tables below list the elements required for the SDLC. Elements do NOT require separate documents and may be satisfied through a variety of methods depending on size, scope, risk, etc. However elements are combined, approvals must be appropriate for all included elements. Solution dependent authoring and approving responsibilities may be delegated and documented in the Plan or Validation Plan. Additional elements and approvers may be added, as determined by the individual project.

Baseline Elements and Approvals

Baseline elements and approvals are the minimum elements and approvals required for all solutions. Refer to Appendix B for the minimum content required for the elements below.

Elements	Business Rep	Technical Rep
Plan		Create
Requirements	Create	Create
Design / Installation Information (Custom / Configured)		Create
Verification Evidence	Create	
Acceptance Statement	Approve	Create / Approve

SOX Elements and Approvals

Solutions that are subject to SOX regulations are required at minimum to meet Baseline elements and approvals with additional elements and approvals. The following table shows Baseline elements and approvals plus additional elements and approvals specific for SOX solutions. Refer to Appendix B for the minimum content required for the elements below.

Elements	Business Rep	Technical Rep	**BTQA**
Plan	**Approve**	Create/**Approve**	**Approve**
Requirements	Create/**Approve**	Create/**Approve**	**Approve**[1]
Design Specification	Create	Create	
Installation		Create	
Verification Evidence	Create/**Approve**[3]		**Approve**[2]
Traceability		**Create**	
Acceptance Statement	Approve	Create / Approve	**Approve**

1: BTQA approve CRS requirements only and approve the risk assessment for all requirements.
2: BTQA approve verification evidence for CRS requirements only
3: Minimum requirement is one approval from Business, Technical or BTQA

Bold text = additional elements and approvals added to Baseline elements

Validation (GxP) Elements and Approvals

Solutions that are subject to GxP regulations are required at minimum to meet Baseline elements and approvals with additional Validation elements and approvals. The following table shows Baseline elements and approvals plus additional elements and approvals specific for GxP solutions. Refer to Appendix B for the minimum content required for the elements below.

Elements	Business Rep	Technical Rep	**BTQA**	**BUQA (GMP only)**
Validation Plan	**Approve**	Create/**Approve**	**Approve**	**Approve**
Requirements	Create/**Approve**	Create/**Approve**	**Approve**[1]	**Approve**
Design Specification		Create/**Approve**		
Installation / **Verification**		Create/**Approve**		
Environment Acceptance		**Create/Approve**		
Verification Plan	**Create/Approve**[3]		**Approve**	**Approve**
Verification Script (Pre-executed)	**Create/Approve**[3]		**Approve**	
Verification Evidence	Create/**Approve**[3]		**Approve**[3]	
Verification Summary	**Approve**	**Create**	**Approve**[2]	**Approve**
Traceability		**Create**	**Approve**	
Acceptance Statement	Approve	Create / Approve	**Approve**[4]	**Approve**
Validation Summary	**Approve**	**Create**	**Approve**	**Approve**

1: BTQA approve CRS requirements only and approve the risk assessment for all requirements.
2: BTQA approve verification evidence for CRS requirements only
3: Minimum requirement is one approval from Business, Technical or BTQA
4: BTQA approval required for GCP and GLP solutions only.

Bold text = additional elements and approvals added to Baseline elements

For GxP Solutions, prior to moving from one process step to the next, any deviation(s), including incomplete items, shall be documented and assessed to determine the impact on the subsequent steps.

For GxP solutions that are deemed to be Software Medical Devices (SMD), refer to CP 904 Software Medical Device Corporate Policy and Procedure.

APPENDIX B ELEMENT COMPONENTS

Each section of Appendix B lists the minimum required element and their components for all solutions and any additional elements and or element components required for solutions categorized as SOX or Validation (Components highlighted in the following tables).

1) Plan or Validation Plan Element

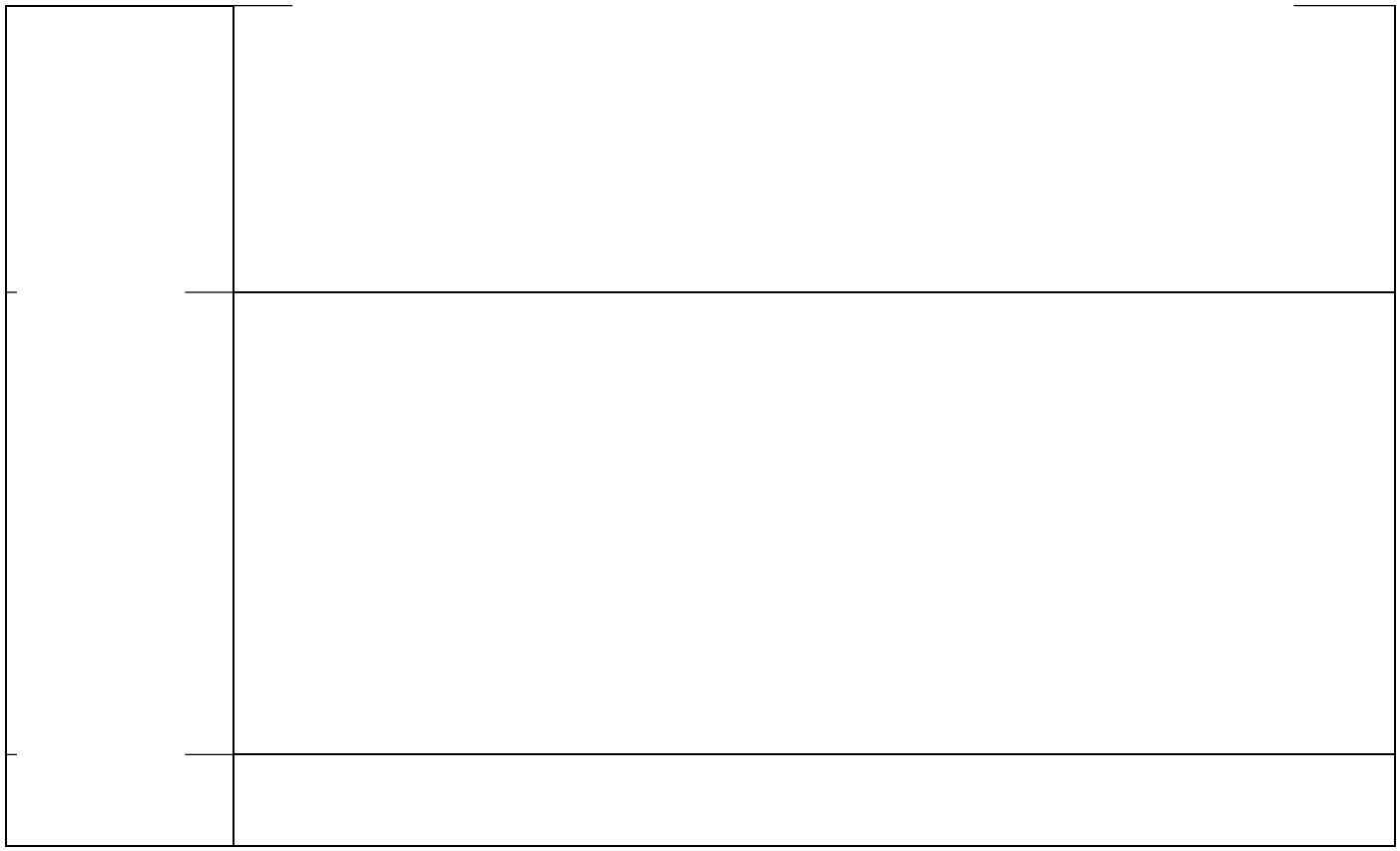
Component:	Characteristics for Consideration
Purpose	Define the objective for the plan.
Intended Use	List the business process that the solution will satisfy.
Scope	Describe the defined boundaries of the project including deployment activities.
Roles & Responsibilities	Identify the roles and responsibilities for planning, and executing the project, including whether BTQA/ BUQA roles are required (based on Compliance Domains). Identify the roles and responsibilities for site / region deployments.
Solution Profile	Document the results of the Solution Profile activity, specifically identifying the applicable compliance domains.
Deliverables List	The elements that will be prepared to demonstrate that the solution will be fit for its intended use including the verification strategy. Refer to Appendix A.
Vendor Assessment *(Required for Validation. Baseline and SOX based on risk)*	Vendor documentation may be leveraged when the vendor has undergone a successful vendor assessment (e.g. Vendor Compliance Assessment Services) and obtained an acceptable rating from Pfizer. Summarize the results of the vendor assessments, and the impact on the requirements risk assessment. The assessment method chosen (e.g. audit, questionnaire) shall be based on a risk assessment considering the criticality and complexity of the system, the service provided by the vendor and prior experience with the vendor.
Verification Strategy	Document the Verification strategy for the Solution, including the verification environments, test methodology, roles required, and the expected documentation output.
Strategic development / deployment approach	1) Determine if deployments will require/allow local configuration of the solution. 2) Deployment model e.g. phased approach, and the data migration strategy. 3) Determine whether the solution will deliver local language capability. 4) Additional characteristics specific to the solution or deployment scope.
Training Impact	Assess and document audience and training requirements for both IT support resources and impacted clients; plan training and documentation as appropriate.
Support (Short Term/Long Term/Service Level Agreement)	Describe the process to manage support through the deployment and into "Business As Usual" (BAU). This may address special support mechanisms immediately following certification, transition to BAU support and expected service levels. It may also include more than technical support (business ownership, help desk, etc.). Support requirements may have been generated from the Common Requirements Set.
User Access	Identify user access methodology (whether new, transitional, or continuing).

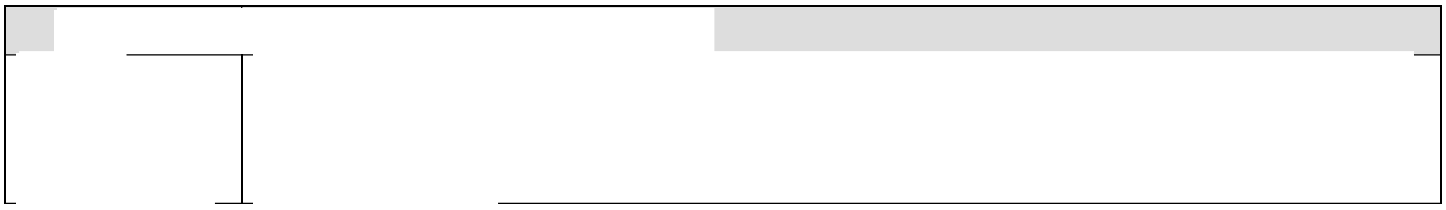
In addition to the above, the following components are also required for **SOX** and **Validation**.

Component:	Characteristics for Consideration
SOP Impact	Describe how procedural controls will be evaluated to determine what modifications, if any, will be needed. Generally this includes reviewing SOPs impacted by the change, determining if the change requires the creation, modification or retirement of procedural controls, and the responsible role for making any required changes
Data Migration	Define the strategy to be used for the verification of data. Consider the following in the data verification process: • Evaluate the risk of the data to be migrated based on business criticality, regulatory requirements, migration complexity and tool qualification. • Define the rigor of the verification of the data and evidence based on the risk Define required elements to document the data verification such as data verification plan to cover the scope of data migration, design document to cover data mapping/conversion, verification test scripts and verification summary report.
Data Integrity Impact	Describe how Data Integrity will be addressed including where applicable: • Identifying the GxP electronic records satisfied by the application • Identifying the GxP electronic signatures satisfied by the application • Assessment of how or if the application has an audit trail for the GxP record and if it can be enabled • Assessment of how or if the application allows the GxP record to be deleted, modified or version controlled
Site Specific Activities	Document as applicable activities that the site are responsible for such as appropriately tested business continuity planning, training and site validation documents.

2) Requirements Element

Component:	Characteristics for Consideration
User Requirements	Describe the needs of a stakeholder, including regulatory requirements, and how that stakeholder will interact with a solution. User requirements bridge business needs and solution requirements. They are developed and defined through requirements analysis.
Solution Requirements	Describe the characteristics of a solution that meet user requirements. Developed and defined through requirements analysis. They include these categories: • Functional Specifications describe the behavior and information that the Solution will manage, including where applicable the use of audit trail (electronic record) and/or electronic signature. They describe capabilities the system will be able to perform in terms of behaviors or operations—specific information technology application actions or responses. • Non-Functional Specifications capture conditions that do not directly relate to the behavior or functionality of the solution, but rather describe environmental





The following Design documentation components are required for **SOX and Validation** only.

Component:	Characteristics for Consideration
Coding Standards	Project teams that have access to code, make changes or use other programs to develop interfaces or external functionality are subject to coding standards. Code must be documented to the extent necessary to follow the logic of the code. If a common Coding Standards SOP exists across project teams, it may be utilized, Coding Standards must address good code design practices, how to identify potential coding vulnerability, malicious code, or other code-related issues.
Design Specification	Details the specifications for hardware, network architecture, database design, screens, programs and interfaces. It typically includes details regarding the hardware and software, operating systems, system requirements, performance requirements, security requirements, standards compliance, procedural control, development methods and detailed system design.
Configuration Specification	Details the functional configuration settings of a system when the application is configured to meet the user requirements and functional specifications.
Technical Architecture	Technical Architecture is the documentation of system architecture specification and physical configuration based upon user needs, the solution, and Pfizer approved technology.
Installation Instructions	Installation Instructions provide the detailed information and orderly steps necessary to install, configure, verify and prepare the system for use.
Configuration Verification	Configuration Verification confirms that the configuration of the system is consistent with the configuration documentation. This verification may be achieved through the execution of the configuration documentation.

The following Installation components are required for **Validation** only.

Component:	Characteristics for Consideration
Installation Verification	Installation Verification confirms that the system is installed correctly per the Installation Instructions. This verification may be achieved through the execution of the Installation Instructions.
Design Verification	Design Verification is an activity of review and confirmation that a solution will satisfy its defined requirements and specifications. The Design Verification activity is performed by subject matter experts and includes review of business process, requirements and specification documentation and regulatory requirements against solution design.
Code Review	Document Code Reviews for customizations against the Coding Standard for GxP solutions. Applicable coding standards, design documents, and code review checklist are used as a basis for the review and the results reported.

4) Environment Acceptance Element

The following components are required for **Validation** only.

Component:	Characteristics for Consideration
Environment Acceptance	Verification of infrastructure (e.g., Mid-Tier, DBs, etc.) activities performed prior to Solution installation such that a controlled environment can support the installation of the Solution.

5) Verification Plan Element

The following components are required for **Validation** only.

Component:	Characteristics for Consideration
Scope	Describe the boundaries of the verification effort.
Assessment Outcomes	Document the Requirements Risk Assessment outcomes, particularly the raising or lowering of risk levels based on risk influencers.
Verification Strategy	Describe the verification strategy that will be used to demonstrate that the solution is fit for intended use.
Elements and Approvals	List elements to be created to support the verification, including their approvals.
Environment	Indicate the verification environment that final or formal testing is performed in and where testing is used to verify that the system is designed, developed and verified against approved specifications and is fit for operational use.
Acceptance Criteria	Define the acceptance criteria that when met will ensure that the solution being delivered meets requirements and is fit for its intended use.
Roles & Responsibilities	List roles and associated responsibilities for the overall verification effort, considering testers, reviewers, and those who will be involved in Exception/Deviation resolution.
Testing Tools	Identify any testing tools that will be used in the overall verification effort. Testing tools must be qualified for Validated solutions.

6) Verification Script (pre-executed) Element

The following components are required for **Validation** only.

Component:	Characteristics for Consideration
Verification Scripts	Based on Appendix C of this procedure and considering the Test Model to be used: 1) Elements of testing must include: a) Objective (e.g., requirements, functions, business processes, or configurations) b) Pre-requisites, Set-Up, and References (if applicable) 2) If performing verification using detailed functional testing instructions: a) Steps or Instructions or specific items being verified. For each Step or Instruction, an expected result, means to record pass or fail, means to attest to the verification result (e.g., tester initial and date), means to record or confirm an actual result, and means to record additional evidence, verification exceptions/deviations, or comments are required. b) "Pass" indicates the observed result after executing the function is equivalent to that specified in the requirement. "Fail" indicates the observed result after executing the function is not equivalent to that specified in the requirement. 3) If performing verification without detailed functional testing instructions: a) Testers must be subject matter experts as demonstrated through training and experience in both the business process and the Solution. The requirement Verification requires that testers have the knowledge to perform the necessary functionality to attest to its correctness without the need for detailed instructions or test scripts. b) Requirements are written as expected results so as to give meaning to attestation. In addition, means to record pass or fail, means to attest to the verification result (e.g., tester initial/date), and means to record additional evidence, verification exceptions/deviations, or comments are required.

7) Verification Evidence Element

Component:	Characteristics for Consideration
Verification Evidence	Perform test execution as detailed in the plan / verification script. Refer to Appendix C of this document for the Testing Evidence Model. Review the executed test and outputs (attachments) and document test status. Ensure testing meets good documentation practice requirements as per SOP SOP-0001

8) Verification Summary Element

The following components are required for **Validation** only.

Component:	Characteristics for Consideration
Scope	Identify the Verification Plan execution being summarized.
Verification Results Summary	Explain variations from the Plan, Verification Exceptions and Deviations, and the overall results.
References	Identifiable references to executed documents/tests and evidence.

9) Traceability Element

The following components are required for **SOX and Validation** only.

Component:	Characteristics for Consideration
Traceability Requirements	Traceability should be documented between user and solution requirements and from solution requirements to design and verification. Traceability can be demonstrated through identifiers/references, electronic trace management tools or traceability matrices.

10) Acceptance Statement Element

Component:	Characteristics for Consideration
Certification of Fitness for Intended Use (Baseline and SOX only)	1. Identify the solution. 2. Certify that the solution is fit for its intended use. 3. Identify the persons making the certification. 4. Document summary statement and/or reference to elements. 5. Document status against Plan requirements including any plan deviations. Approval of the Acceptance Statement element for Baseline verifies that all required elements have been created in accordance with this procedure.

The following components are required for **Validation** only.

Component:	Characteristics for Consideration
Declaration of Validation	1. Identify the solution and applicable GxP regulatory domains. 2. Declare that that there is a high degree of assurance the solution will consistently operate in accordance with predetermined specifications and is therefore Validated, and Certified for its Intended Use. 3. Identify the persons making the Declaration. 4. Identify where the project summary of activities and deliverables is located (not necessary if combined with summary element). This Declaration may be included with other elements such as the Validation Summary.

11) Validation Summary Element

This element and its components are required for **Validation** only.

Component:	Characteristics for Consideration
Purpose	To demonstrate that all criteria has been met, per the Validation Plan, to release the solution for operational use.
Scope	Clearly identify the plan that this document is summarizing execution against.
Summary of Activities / Deliverables	List activities and deliverables required in the Validation Plan. Identify all final documents by document reference and/or name.
Variations from the Plan	Document any changes or deviations from the Validation Plan. Include justification for each change. Corrective actions taken or corrective action plans must be reviewed and approved prior to, or concurrent with, approval of the Validation Report
Operations & Maintenance	Outline Operation and maintenance procedures used to ensure the solution will be maintained in a compliant state.
CRS Disposition	Document the CRS disposition including any deviations or provide a reference to a CRS disposition document.

APPENDIX C VERIFICATION STRATEGY

Rigor of verification and required evidence is based on the requirement's risk rating. Using option 1 or 2 below, the project team should obtain the Requirements criticality rating:

- Option 1: Assign a risk rating to be used for all the requirements.
- Option 2. Determine Risk Rating for each requirement or group of requirements. Assign each requirement or group of requirements the appropriate risk rating.

Using the Requirement Criticality Rating and Classification, identify the corresponding Requirement Risk Rating using the matrix below.

		Requirement Classification		
		Custom	Configured	NonConfigured
Requirements Criticality Rating	High	Intensive	Intensive	Standard
	Medium	Intensive	Standard	Standard
	Low	Minimal	Minimal	Minimal

Identify the requirement classification

Requirement Classification	Definition
Non-Configured	Functionality is provided by the off-the-shelf solution. The functionality does not require any additional customization or configuration to support business processes, or the default configuration is used.
Configured	Functionality required specification and configuration other than default settings to support specific business processes. Software code is not altered.
Custom	Functionality is developed through code development or modification in-house or by a contracted supplier based on defined requirements.

Identify the requirements criticality

Criticality	Definition
High	**CTB** - Critical to Business – Requirements (not including GxP) without which the business would be unable to achieve business objectives. Includes components that create or maintain vital records. Examples include, but are not limited to: • The requirement functionality is required to maintain revenue. • The requirement functionality would shut down critical Pfizer business processes if the solution failed. **CTQ** – Critical to Quality – Requirements that are directly related to product quality, patient safety or data integrity. Examples include, but

	are not limited to: • The requirement functionality is required in the event of a product recall. • The requirement functionality is involved in the transfer of data to a Board of Health • The requirement functionality supports adverse event data (Pharmacovigilence) • An electronic signature requirement for a business process that is critical to quality will be assessed as High. (e.g., Quality Professional (QP) dispositioning a lot or electronic batch records.)
Medium	Requirements that do not impact CTQ or CTB functionality of the solution but are governed by internal regulations or external regulations. Note: This includes GxP requirements that are not CTQ For GxP systems, Electronic Record and Electronic Signature Requirements are classified as Medium criticality with the exception of electronic signature requirement that are critical to quality as stated above under the High criticality definition.
Low	Not High or Medium criticality

Risk Influencers

Risk influencers are factors that may justify increasing or decreasing the Requirement Risk Rating. If used, risk influencers must be documented along with the justification for the change in Requirements Risk Rating. Unless otherwise justified, risk influencers increase or decrease the risk rating by one level only. Following are examples of risk influencers and how they might influence the Requirements Risk Rating.

Solution novelty
The newness of the solution to the industry and/or to Pfizer may justify altering the Requirement Risk Rating. If the solution is well-established and supported in Pfizer, that may justify decreasing the Requirement Risk Rating a level (e.g. intensive to standard). Conversely, the Project Team may increase the Requirement Risk Rating a level (e.g. minimal to standard) if the solution is new to Pfizer and the industry.

Vendor status
The vendor assessment outcome and history with Pfizer may justify altering the Requirement Risk Rating. If the vendor supplying the solution has been assessed as acceptable by Pfizer, that may justify decreasing the Requirement Risk Rating a level (e.g. from standard to minimal). Conversely, a new vendor may justify increasing the Requirement Risk Rating a level.

Verification Rigor and Evidence

Verification evidence is used to prove that verification activities took place and the solution demonstrates fitness for intended use, has been properly installed, and operate correctly. Rigor of verification and required evidence is based on each individual requirement's risk rating. Each rating and its verification requirements are summarized in the table below and detailed in the following section.

Verification documentation requirements are detailed in Appendix A. Validation requires Verification Scripts pre-approved prior to testing. Baseline and SOX Solutions do not require pre-approved verification scripts however verification evidence must be provided that shows testing has been completed successfully. The approach to verification including use of electronic test tools must be documented in the Plan (or Validation Plan).

<table>
<tr><th>Minimal (M)</th><th>Standard (S)</th><th>Intensive (I)</th></tr>
<tr><td rowspan="4">Tester attestation</td><td></td><td>Aggressively challenge functionality</td></tr>
<tr><td colspan="2">Test instructions and acceptance include testing steps</td></tr>
<tr><td colspan="2">Objective evidence of testing</td></tr>
<tr><td colspan="2">Pass/Fail with tester attestation</td></tr>
</table>

Minimal testing can be used for functionality that is not subject to internal or external regulations and is not considered critical to business. Minimal verification relies on a tester documenting that testing has been satisfactorily completed to demonstrate that solution functionality is fit for its intended use as per the documented requirements. Evidence of satisfactory test completion is provided in the form of recording the tester(s) initials and date or capturing the tester(s) identity and date of testing in an electronic tool. Additional evidence such as screen shots or detailed recording of actual outcomes during testing is not required.

Minimal verification can also utilize a combination of previously performed iterative or development testing and the leveraging of an acceptable vendor quality system in place of final verification execution. In this situation it is sufficient to record in the verification documentation that the vendor testing is being leveraged and no further action is required.

For SOX and Validation, a vendor quality system can only be leveraged when the vendor has obtained an acceptable assessment rating. Minimal can be leveraged for non-configured requirements only.

Results of the testing must be documented as per the Plan.