IT Change Management for GxP Environment

1. **PURPOSE**:

   1.1. This Standard Operating Procedure (SOP) details the process for managing changes to IT systems pertinent to GxP activities. It ensures all IT changes go through an approval process, ensuring that systems supporting regulated activities do not cause unintended disruption to business operations.

2. **SCOPE**:

   2.1. This SOP applies to changes affecting IT systems at Company's facility in North Carolina that have the potential to disrupt the technical environment, including data integrity, system availability and validation, continuity of operations, regulatory compliance, and record traceability.

3. **DEFINITIONS AND ABBREVIATIONS:**

Table 3-1: Definitions and Abbreviations

Term/Abbreviation	Description
Backout Plan	A predetermined plan, a set of steps, to revert or undo a change if the implementation causes issues or problems. A backout plan ensures that a system can return to a prior stable state.
Corrective Action/Preventative Action (CAPA)	Action(s) identified to address situations that may have significant potential or actual impact on safety, quality, or efficacy of the product. Corrective actions eliminate the cause of a detected, previously occurring non-conformity or other undesirable situation. Preventative actions eliminate the cause of a potential non-conformity or other undesirable potential situation that has not yet occurred.
Change	Any addition, modification, or removal of components that influence system performance, functionality, or working methods for IT systems, including but not limited to defects, bug fixes, upgrades, or enhancements.
Change Owner	The individual accountable for a change. This includes ensuring all approvers have contributed to and approve the change plan, developing the change plan for implementing the change, monitoring and managing actions designed to ensure progression in a timely manner.
Change Request (CR)	A documented proposal to introduce a change. A change request is typically used to request evaluation, planning, and approval of modifications to an IT system.
Change Review Board	A cross-functional group responsible for ensuring that proposed changes are appropriately defined, technically addressed, and roles and responsibilities determined.
Configuration Change	A modification to a system's configuration settings, parameters or operating environment that may affect system performance or compliance.
Data Integrity (DI)	The extent to which all data are attributable, legible, contemporaneous, original, accurate, complete, consistent, enduring, available, and traceable throughout the data lifecycle. This lifecycle encompasses all stages of data handling from creation and storage to processing, retrieval and disposal.
Deployment	The final step of the IT change management process when the release is introduced into the production environment.
Electronic Signatures	Electronic approvals used on change forms. Validated signatures are required for GMP IT changes.
Emergency Change	A change needed immediately to resolve an issue that is assessed to be high-risk, urgent, cause operational impact. Emergency changes bypass the standard timelines for changes and maintenance schedules but still require Emergency Change Review Board Approval.

Term/Abbreviation	Description
Emergency Change Review Board (E-CRB)	A subset of the Change Review Board that provides decisions for Emergency Changes.
Enhancement	Any change that adds new functionality or changes to the scope of the existing functionality within a system.
Environment	Controlled stages where changes are built, tested, verified, and finally deployed.
Impact Assessment	An evaluation of the potential impact of a proposed change on product quality, safety, and regulatory compliance.
Integration Testing	Testing performed to confirm that a change component exists concurrently and correctly with other integrated systems.
Operational Change	A change that modifies existing functionality or configuration within the system without expanding the scope or introducing new features.
Patch	A set of changes to a computer program or its supporting data designed to update, fix, or improve system performance. This can also include fixing security vulnerabilities.
Patch Maintenance	A scheduled and controlled process for routinely identifying, assessing, and applying patches that vendors provide to operating systems and applications to maintain security, stability, and reliability of IT systems.
Pre-Approved Change	A predetermined, low risk change that proceeds without full CRB review.
Regression Testing	A test that is performed to ensure that new changes do not introduce unexpected problems in components that were previously functioning.
Release	A single change or a collection of changes to be deployed through system environments.
Release Package	A bundle of changes that are built, tested, and deployed in a single release. The changes may be deployed through environments or directly to production.
Request for Change (RFC)	A helpdesk ticket raised with ICT to document an issue, bug, defect, request, or enhancement or service.
Risk-Based Evaluation	An assessment of the likelihood and severity of adverse impacts from a change and mitigating actions to take to reduce the risk.
User Acceptance Testing (UAT)	Testing that is performed to confirm whether changes meet business requirements, workflows, and user needs. User Acceptance Testing typically occurs before production.
Validated State	Documented evidence that a system consistently performs as intended through its lifecycle

4. RESPONSIBILITIES:

4.1. Initiator

4.1.1. Receives request for change through ServiceNow and assigns ticket to the appropriate IT change participants for further assessment

4.1.2. Receives notifications from third-party vendors regarding required patches, updates, or system changes and logs these items as new change requests.

4.1.3. Notifies the Change Owner, SME, ICT Administrator of emergent or expedited change requests.

4.1.4. Communicates preliminary change details to IT change stakeholders via meeting or email.

4.1.5. Refines change requirements with various stakeholders through a meeting or email.

4.1.6. Completes and submits the initial documentation to begin the change process and submits it to the Change Review Board.

4.2. Change Owner

4.2.1. Accountable for the end-to-end oversight, risk control, and regulatory compliance of IT changes that are GxP relevant, from initiation to closure.

4.2.2. Ensures change maintains validated state and preserves data integrity.

4.2.3. Ensures change follows this SOP and all referenced GxP procedures.

4.2.4. Assigns portions of the impact assessment to appropriate SMEs.

4.2.5. Creates the required impact assessment and assigns portions of the assessment to the relevant SMEs to evaluate system, technical, security, validation, or business impacts.

4.2.6. Ensures impact assessment addresses validated state, GxP workflows, data integrity (ALCOA+) electronic records and audit trails, interfaces, and integrations.

4.2.7. Based on impact assessment outcomes, determines whether other validation activities or further testing is required.

4.2.8. Ensures that the change plan includes the approved testing approach, rollback and recovery strategy, communication plan, and the implementation window.

4.2.9. Ensures testing scope aligns with system criticality, GAMP category, and patch and vulnerability outputs.

4.2.10. Confirms that test evidence is defined prior to approval.

4.2.11. Monitors change execution against approved plans.

4.2.12. Reviews completion evidence and approved the change closure, subject to QA approval as required.

4.2.13. Ensures all information appended to the change record is accurate, complete, and traceable.

4.3. System Owner

4.3.1. Confirms that changes do not compromise validated state pre and post change implementation.

4.3.2. Ensures that the computerized system operates according to its intended use and supports GxP processes and maintains accountability for the systems intended use.

4.3.3. Ensures the system remains suitable to support regulated business processes.

4.3.4. Provides input to the impact assessment regarding system functionality, business workflows, interfaces, dependencies, and the potential impact to validated use

4.3.5. Confirms that required validation activities, regression testing, or business process verification are appropriate for the system's intended use.

4.3.6. Reviews test results relevant to system functionality and business workflows as applicable.

4.3.7. Reviews patch-driven changes affecting the system and confirms system and business operations compatibility.

4.3.8. Coordinates with the Change Owner and ICT [Administrator/Representative] to support implementation scheduling, user communication, and business readiness.

4.3.9. Reports issues, deviations, or unexpected behavior to the Change Owner.

4.4. ICT Administrator

4.4.1. Executes approved GxP IT changes in accordance with approved plans, procedures, and controls.

4.4.2. Generates objective evidence of implementation and testing activities.

4.4.3. Performs approved change activities as designated with the approved change plan, testing protocol, and implementation schedule.

4.4.4. Implements changes after approvals have been obtained.

4.4.5. Performs technical testing, verification activities and system checks as defined in approval test plans or protocols.

4.4.6. Implements patch-driven changes in alignment with the approved change record, Patch and Vulnerability SOP, and vendor instructions.

4.4.7. Ensures system backups or recovery measures are completed prior to implementation as necessary.

4.4.8. Verifies system availability and functionality after implementation.

4.4.9. Supports post-implementation review activities by providing requested technical evidence or clarifications.

4.4.10. Ensures implementation and testing evidence is provided to the Change Owner for inclusion in the change record.

4.4.11. The ICT Administrator does not approve the change.

4.5. Business Lead

4.5.1. Provides business process input to ensure GxP IT changes are planned and implemented with appropriate consideration of operational impact, user readiness, and business continuity.

4.5.2. Provides input of potential impact a change has on GxP business processes, operational workflows, user activities, and scheduling.

4.5.3. Identifies business constraints, dependences, or timing considerations.

4.5.4. Supports communication plan development for impacted users and stakeholders.

4.5.5. Assists in coordinating business readiness activities related to a change such as user notifications, training, and procedural updates.

4.5.6. Coordinates with the Change Owner and system Owner to ensure business operations are prepared for implementation activities.

4.5.7. Confirms the available of business resources during implementation windows.

4.6. Validation Representative

4.6.1. Provides subject matter expertise on validation requirements to ensure GxP IT changes are assessed, tested, and documented appropriate to system risk, intended use, and regulatory expectations.

4.6.2. Assesses system intended use, GAMP category, and impact to validation functions, electronic records, audit trails, or data integrity.

4.6.3. Provides recommendations on the type and extend of validation activities that are required.

4.6.4. Advises on appropriate testing approaches, including regression testing, qualification activities, or targeted verification as applicable.

4.6.5. Reviews validation-related test plans, protocols, or evidence to confirm alignment with validation expectations.

4.6.6. Reviews validation documentation generated as part of changes to confirm completeness and traceability.

4.6.7. Identifies gaps or deficiencies requiring remediation prior to the change approval or closure.

4.6.8. Does not approve change execution, closure, or GxP acceptability.

4.6.9. Does not override Quality Assurance decisions.

4.7. Quality Assurance

4.7.1. Ensures GxP IT changes are properly assessed, controlled, tested, documented, and approved in accordance with regulatory requirements.

4.7.2. Ensures that the validates state and data integrity are preserved.

4.7.3. Independently oversees GxP IT changes to ensure compliance with applicable regulations, internal procedures, and quality standards.

4.7.4. Ensures the segregation of duties throughout the change lifecycle.

4.7.5. Reviews GxP Impact Assessments to confirm the following:

4.7.5.1. Risks to product quality, patient safety, and data integrity have been appropriately identified.

4.7.5.2. Validation and testing recommendations are commensurate with risk.

4.7.6. Challenges assessments where necessary to ensure adequate controls are applied.

4.7.7. Approves GxP IT changes prior to implementation.

4.7.8. Approves validation approaches and testing adequacy from the perspective of compliance and may withhold approval if GxP risks are not properly addressed.

4.7.9. Reviews completed change records to confirm the following:

4.7.9.1. All required testing and validation activities are completed.

4.7.9.2. Deviations are appropriately addressed.

4.7.9.3. Effectiveness checks were performed when required.

4.7.10. Approves the final closure for GxP IT changes.

4.7.11. Reviews emergency GxP IT changes retrospectively to confirm appropriateness of emergency classification, risk mitigation adequacy, and the completion of required follow-up actions.

4.8. IT Change Review Board

4.8.1. Provides cross-functional governance oversight for GxP IT changes to ensure that risks, impacts, dependencies, and implementation considerations are evaluated and aligned prior to execution.

4.8.1.1. The IT Change Review Board is comprised of the System Owner, ICT Administrator, Quality Assurance, Validation, Business Lead, Release Management Analyst, and the Change Owner.

4.8.2. Reviews GxP IT changes that are high-risk, cross-system or cross-functional, driven by patches with elevated impact, and operationally or technically complex.

4.8.3. Ensures that proposed changes are aligned with business priorities, risk tolerance, and implementation constraints.

4.8.3.1. Reviews impact assessments and risk evaluations to confirm the following risks are understood, mitigation is underway, and the proposed testing and validation approaches are proportionate.

4.8.4. Provides recommendations or conditions for proceeding, deferring, or planning changes.

4.8.5. Reviews implementation windows and sequencing to identify conflicts with other changes, resource constraints, and business or operational risks.

4.8.6. Supports change coordination across systems and teams.

4.8.7. Provides an escalation forum when risk acceptance decisions are required, conflicts arise between stakeholders, and deviations from standard change pathways are proposed.

4.8.8. Escalates unresolved compliance concerns to Quality Assurance as required.

4.8.9. Emergency Change Review Board (E-CRB)

4.8.9.1. A CRB subset that provides expedited governance oversight for emergency GxP IT changes that must be implemented to address immediate risks to system availability, security, data integrity, or patient safety.

4.8.9.2. Reviews and authorized emergency GxP IT changes when standard change timeliness cannot be followed.

4.8.9.3. Confirms the emergency classification is appropriate and justified.

4.8.9.4. Reviews known risks associated with expediated implementation.

4.8.9.5. Confirms reasonable risk mitigation or compensating controls are in place.

4.8.9.6. Requires that emergency changes undergo retrospective impact assessment, validation review, and QA review and approval.

4.8.9.7. Ensures emergency changes are documented in accordance with this SOP and related procedures.

4.9. Subject Matter Expert

4.9.1. Provides specialized technical or process expertise to support impact assessment, planning, testing, and issue resolution activities for GxP IT changes as requested by the Change Owner.

4.9.2. Provides technical or functional expertise related to system architecture, configuration, integrations, data flow, or business processes.

4.9.3. Supports the evaluation of potential risk impacts to system functionality or workflows.

4.9.4. Contributes technical input to impact assessments, including but not limited to configuration implications, interface dependencies, and performance considerations.

4.9.5. Does not determine the overall GxP impact or validation requirements.

4.9.6. Assists with the development or the execution of technical testing activities when required.

4.9.7. Supports troubleshooting and resolution of issues identified during testing or implementation.

5. PROCEDURE:

5.1.1. Change Categorizations

5.1.1.1. Determination

5.1.1.1.1. A change is determined to be applicable under the IT Change Management SOP if the change affects any of the following:

5.1.1.1.1.1. IT systems that support GxP activities

5.1.1.1.1.2. Data Integrity

5.1.1.1.1.3. System availability, operational continuity, or validated state

5.1.1.1.1.4. Regulatory compliance with inspection readiness

5.1.1.1.1.5. Traceability of GxP records

5.1.1.2. Routine Change

5.1.1.2.1. A pre-approved and low risk change to a GxP system that is repeatable and performed in accordance with an established and approved method.

5.1.1.2.2. Follows a streamlined approval and assessment process, which is defined in this SOP and approved by QA.

5.1.1.2.3. Routine Changes meet all of the following criteria:

5.1.1.2.3.1. Evaluated and approved for standard execution.

5.1.1.2.3.2. Does not alter the system’s intended use.

5.1.1.2.3.3. Does not introduce new functionality.

5.1.1.2.3.4. Does not impact validated state, data integrity, or GxP workflows beyond predefined conditions.

5.1.1.2.3.5. Follows documented procedures with predefined testing and acceptance criteria.

5.1.1.3. Normal Change

5.1.1.3.1. A planned change to a GxP system that requires full assessment, planning, approval, and documentation. Normal changes include but are not limited to the following:

5.1.1.3.1.1. Changes to configuration.

5.1.1.3.1.2. Upgrades or enhancements to systems.

5.1.1.3.1.3. Changes that affect the functionality of a system or workflows.

5.1.1.3.1.4. Change that require validation or regression testing.

5.1.1.3.2. A normal change does not qualify as a routine change or an emergency change.

5.1.1.3.3. Normal changes follow the full change lifecycle as defined in this SOP.

5.1.1.4. Emergency Change

5.1.1.4.1. An emergency change is one that must be implemented immediately to address an emergent, immanent risk to system availability, data integrity, system security, patient safety, or the continuity of regulated operations.

5.1.1.4.2. Emergency changes must include documented justification for the emergency classification, authorization by the E-CRB, and implementation of risk mitigation or compensating controls.

5.1.1.4.3. All emergency changes undergo retrospective review, including an impact assessment, validation evaluation if applicable, and receiving QA approval.

5.1.1.5. Patch-Driven Change

5.1.1.5.1. A patch-driven change is a change that has been initiated as a result of applying patches, updates, or remediations to systems supporting GxP activities.

5.1.1.5.1.1. All patch-driven changes that impact GxP activities must include a documented GxP impact assessment, determination of validation and testing requirements, and required approvals prior to implementation.

5.1.1.5.2. Patch-driven changes may include operating system patches, application or database patches, security remediations, or updates to firmware or infrastructure that impact GxP systems.

5.1.1.5.3. A patch-driven change may be classified also as a routine normal, or emergency change depending on risk, impact, and urgency.

5.1.2.Change Lifecycle

5.1.2.1. All IT changes affecting GxP processes follow the change lifecycle defined in this SOP. Changes must progress to each phase sequentially unless classified as an emergency change.

5.1.2.2. Initiation

5.1.2.2.1. Change initiation does not imply approval or authorization to implement the change.

5.1.2.2.2. Initial inputs include ServiceNow, vender notifications, vulnerability findings, and audit findings. Changes may also be initiated due to the following:

5.1.2.2.2.1. The identification of a system deficiency or improvement opportunity.

5.1.2.2.2.2. Patch or vulnerability management activities.

5.1.2.2.2.3. System updates

5.1.2.2.2.4. Inspection observations or CAPAs

5.1.2.2.3. Each initiated change includes at least a clear description of the proposed change, identification of impacted systems, preliminary indication of GxP relevance, and the reason for the change.

5.1.2.2.4. The outcome of initiation is a documented change record that is eligible for GxP applicability determination, change classification, and an impact assessment.

5.1.2.2.5. The initiator assigns a Change Owner before proceeding to the next step.

5.1.2.3. Impact Assessment

5.1.2.3.1. IT changes undergo a documented impact assessment prior to planning, approval, or implementation unless otherwise justified under the Emergency Change process.

5.1.2.3.2. Ownership

5.1.2.3.2.1. The Change Owner is responsible for ensuring the impact assessment is performed and documented.

5.1.2.3.2.2. The assessment may be supported by input from the System Owner, ICT Administrator, SMEs, Validation Representative, or Business Lead.

5.1.2.3.2.3. Quality Assurance reviews the completed assessment and confirms adequacy and completeness.

5.1.2.3.3. Scope

5.1.2.3.3.1. The impact assessment evaluates the potential impact of the following areas as applicable. Other areas may be included as necessary.

5.1.2.3.3.1.1. Validated State and Intended Use

5.1.2.3.3.1.1.1. Determine whether the change effects validated functions or system intended use and identifies whether requalification, qualification, or regression testing may be required.

5.1.2.3.3.1.2. GxP Business Processes

5.1.2.3.3.1.2.1. Determine the impact to regulated workflows, process execution, procedural controls, or user interactions.

5.1.2.3.3.1.3. Electronic Records and Data Integrity

5.1.2.3.3.1.3.1. Determine the impact to electronic records, audit trails, electronic signatures, data accuracy, completeness, consistency, or traceability.

5.1.2.3.3.1.4. System Interfaces and Dependencies

5.1.2.3.3.1.4.1. Determine the impact to upstream or downstream systems, integrations, shared infrastructure, or data transfers.

5.1.2.3.3.1.5. Security and Access Controls

5.1.2.3.3.1.5.1. Determine the impact to authentication, authorization, segregation of duties, and security controls supporting GxP activities.

5.1.2.3.3.1.6. Availability and Business Continuity

5.1.2.3.3.1.6.1. Determine the impact to system availability or continuity of operations.

5.1.2.3.3.1.6.2. Identifies the potential for operational disruption affecting regulated activities.

5.1.2.3.4. Controls

5.1.2.3.4.1. Impact assessments must be completed prior to change approval.

5.1.2.3.4.2. Changes may not proceed to implementation without an approved impact assessment.

5.1.2.3.4.3. Disagreements regarding impact or required controls must be escalated to the CRB or Quality Assurance.

5.1.2.3.5. Outcomes

5.1.2.3.5.1. Impact assessment outcomes include documented conclusions about the overall GxP relevance of the change, the level of risk introduced by the change, the need for validation or enhanced testing.

5.1.2.3.5.2. Impact outcomes shall not be downgraded for scheduling, resource, or operational convenience.

5.1.2.3.5.3. The outcomes also include approvals, oversight level, and whether an effectiveness check is required.

5.1.2.3.5.4. No impact

5.1.2.3.5.4.1. The “No Impact” outcome is assigned with the assessment concludes the following about the involved change:

5.1.2.3.5.4.1.1. No impact to validated functions or the system’s intended use.

5.1.2.3.5.4.1.2. No impact to GxP business processes.

5.1.2.3.5.4.1.3. No impact to electronic records, audit trails or data integrity.

5.1.2.3.5.4.1.4. No introduction of new functionality or configuration that affects GxP use.

5.1.2.3.5.4.2. Changes with no impact do not require validation, and testing may be limited to basic technical or functional verification.

5.1.2.3.5.4.3. QA review and approval are still required prior to implementation.

5.1.2.3.5.5. Minor Impact

5.1.2.3.5.5.1. The “Minor Impact” outcome is assigned with the assessment concludes the following about the involved change:

5.1.2.3.5.5.1.1. Limitedly impacts GxP systems or workflows.

5.1.2.3.5.5.1.2. System intended use is not altered.

5.1.2.3.5.5.1.3. Data integrity and regulatory compliance are not compromised.

5.1.2.3.5.5.1.4. Targeted testing or limited regression testing may be required.

5.1.2.3.5.5.2. Validation activities may be limited in scope and targeted to only affected functions.

5.1.2.3.5.5.3. Testing requirements must be proportionate to the identified risk.

5.1.2.3.5.5.4. Effectiveness checks may be required depending on the risk and the type of change.

5.1.2.3.5.5.5. QA approval is required prior to implementation.

5.1.2.3.5.6. Major/Validation-Level Impact

5.1.2.3.5.6.1. The “Major Impact” outcome is assigned with the assessment concludes the following about the involved change:

5.1.2.3.5.6.1.1. Impacts validated functions or system intended used.

5.1.2.3.5.6.1.2. Introduces new or modified functionality supporting GxP activities

5.1.2.3.5.6.1.3. Can potentially impact electronic records, audit trails, or data integrity.

5.1.2.3.5.6.1.4. Requires formal validation, qualification, or extensive regression testing.

5.1.2.3.5.6.2. Formal validation activities are required.

5.1.2.3.5.6.3. Validation plans, protocols, and evidence must be defined prior to approval.

5.1.2.3.5.6.4. Major Impact IT changes require enhanced oversight by QA and the CRB is required.

5.1.2.3.5.6.5. Implementation cannot proceed without documented QA approval of the validation approach.

5.1.2.4. Risk Assessment

5.1.2.4.1. This SOP governs when and why change-specific risk assessment procedures are required; however, the methodologies ranging from formal to informal risk assessments shall be performed according to the following SOPs:

5.1.2.4.1.1. KK-QD-128633: Data Integrity Risk Assessment Process

5.1.2.4.1.2. KK-QD-144070: Sanford Site Quality Manual

5.1.2.4.2. Requirements

5.1.2.4.2.1. A risk assessment must be performed when a change is determined to have Minor or Major/Validation-Level Impact.

5.1.2.4.2.2. The risk assessment may be waved when a change is determined to have No Impact.

5.1.2.4.2.3. In all cases, a justification for the presence or absence of a required risk assessment must be produced by the Change Owner and reviewed by QA.

5.1.2.4.3. Ownership

5.1.2.4.3.1. The Change Owner is responsible for the risk assessment but may be supported by the Validation Representative, ICT Administrator, Subject Matter Experts, and the System Owner.

5.1.2.4.3.2. Scope

5.1.2.4.3.3. QA reviews the risk assessment to determine completeness, adequacy, and appropriateness.

5.1.2.4.3.4. The risk assessment evaluates risks pertaining to the change including:

5.1.2.4.3.4.1. Validated state and intended system use

5.1.2.4.3.4.2. Data integrity risk

5.1.2.4.3.4.3. Risk to good documentation practices, including electronic records, audit trails, or electronic signatures.

5.1.2.4.3.4.4. System availability and business continuity of GxP operations

5.1.2.4.3.4.5. Failure, misconfiguration, or unintended consequence risks.

5.1.2.4.3.5. The risk assessment must consider both the likelihood of occurrence as well as the potential severity of the impact to GxP activities identified from the Impact Assessment.

5.1.2.4.4. Controls

5.1.2.4.4.1. Risk assessments are conducted before a change is approved.

5.1.2.4.4.2. Risk assessments must be reviewed by QA.

5.1.2.4.4.3. If a risk is determined to be unacceptable, the change will be replanned with additional controls or mitigations or escalated to the CRB for resolution.

5.1.2.4.5. Outcome

5.1.2.4.5.1. The risk assessment results serve as a resource to confirm or refine testing and validation requirements, identify necessary risk controls and mitigations, and inform approval and oversight decisions.

5.1.2.4.5.2. The risk assessment is also resource to help determine whether an Effectiveness check is required.

5.1.2.5. Planning and GxP Risk Controls

5.1.2.5.1. The scope and depth of the planning activities must be commensurate with the identified impact and risk level of the change.

5.1.2.5.2. Planning activities must be documented in the change record.

5.1.2.5.3. Ownership

5.1.2.5.3.1. The Change Owner is responsible for the risk assessment but may be supported by the Validation Representative, ICT Administrator, Subject Matter Experts, and the System Owner.

5.1.2.5.3.2. QA reviews planning outputs as part of the change approval process.

5.1.2.5.4. Planning Elements

5.1.2.5.4.1. Planning for GxP IT changes includes the following as is applicable:

5.1.2.5.4.2. Testing and Validation

5.1.2.5.4.2.1. The plan includes what needs to be tested, including:

5.1.2.5.4.2.1.1. A clear definition of required testing activities based upon the impact and risk assessment outcomes.

5.1.2.5.4.2.1.2. References to applicable validation documentation or protocols.

5.1.2.5.4.2.1.3. If applicable, the identification of validation, qualification, or regression testing requirements.

5.1.2.5.4.3. Risk Controls and Mitigations

5.1.2.5.4.3.1. Identification of controls or mitigations required to reduce risk that have been identified.

5.1.2.5.4.3.2. Confirmation that the residual risk is acceptable prior to approval.

5.1.2.5.4.3.2.1. If the residual risk is not acceptable, then the change must be re-planned or escalated.

5.1.2.5.4.3.3. Wherever applicable, documentation of compensating controls.

5.1.2.5.4.4. Rollback and Recovery Strategy

5.1.2.5.4.4.1. The rollback and recovery strategy must include contingency, rollback and recover actions to occur in the event of implementation failure.

5.1.2.5.4.5. Implementation and Planning

5.1.2.5.4.5.1. The implementation approach and sequency must be defined, required resources must be identified, and a proposed implementation window with constraints must be provided.

5.1.2.5.4.6. Communication and Readiness

5.1.2.5.4.6.1. Communication and readiness must include a plan for user communication, training, or procedural updates.

5.1.2.5.4.6.2. A communication plan identifying stakeholder who require notification must be included.

5.1.2.5.4.7. Effectiveness Check Determination

5.1.2.5.4.7.1. The Change Owner determines whether an Effectiveness check is required and QA approves it.

5.1.2.5.4.7.2. An effectiveness check is required when:

5.1.2.5.4.7.2.1. The change is categorized as a Major/Validation-Level impact.

5.1.2.5.4.7.2.2. The change introduces functionality that is new or modified.

5.1.2.5.4.7.2.3. A risk assessment identifies residual or mitigated risks that require confirmation.

5.1.2.5.4.7.2.4. A change is patch-driven but with elevated GxP implications.

5.1.2.5.4.7.2.5. Quality Assurance or the Change Review Board requires it.

5.1.2.5.4.7.3. If a change is determined to have no impact or minor impact, then an effectiveness check is not required.

5.1.2.5.4.7.4. A definition of the effectiveness criteria and timing must be provided.

5.1.2.5.5. Outcomes

5.1.2.5.5.1. The outcome of the planning and risk controls include a defined and documented testing approach, identified risk controls and mitigations, rollback and recovery plan, and readiness for approval review.

5.1.2.5.5.2. No GxP IT change may proceed to approval without completed planning activities commensurate with the impact and risk level.

5.1.2.6. Approval

5.1.2.6.1. All GxP IT changes shall be approved prior to implementation.

5.1.2.6.2. Approval confirms that required assessments have been completed, identified risks are understood and acceptably controlled, required testing and validation activities are defined, and appropriate oversight has been applied.

5.1.2.6.3. Approval authorizes implementation only as dictated by the plan.

5.1.2.6.4. Authority

5.1.2.6.4.1. Approval of GxP IT changes include at least QA to approving GxP acceptability and the Change Owner

5.1.2.6.4.1.1. Additional approvals from the System Owner, Validation Representative, and Change Review Board may be required depending on the change impact and risk.

5.1.2.6.4.2. Documentation Review

5.1.2.6.4.3. Approval decisions are based on the review of documented information. Missing documentation will result in approval being withheld until deficiencies are resolved:

5.1.2.6.4.3.1. Impact Assessment

5.1.2.6.4.3.2. Risk Assessment if required

5.1.2.6.4.3.3. Testing and Validation approach

5.1.2.6.4.3.4. Risk Controls and Mitigations

5.1.2.6.4.3.5. Rollback and Recovery Strategy

5.1.2.6.4.3.6. Effectiveness Check Determination

5.1.2.6.5. Controls

5.1.2.6.5.1. Approvals are documented in the designated change management system (ServiceNow and/or Veeva)

5.1.2.6.5.2. Conditional or partial approvals must be clearly documented with defined conditions.

5.1.2.6.5.3. Changes cannot proceed to implementation without documented QA approval.

5.1.2.6.5.4. Approval authority may not be delegated to individuals responsible for executing the change.

5.1.2.6.5.5. Changes to the approved plan require re-assessment and re-approval.

5.1.2.6.6. Outcome

5.1.2.6.6.1. The outcome of the approval is the authorization to implement the GxP IT change according to the approved change plan.

5.1.2.6.6.2. Approval does not authorize deviations from the approved plan, waive validation or testing requirements, or eliminate post-implementation review obligations.

5.1.2.6.7. Emergency Approval Conditions

5.1.2.6.7.1. Emergency GxP IT changes follow expedited approval pathways identified in section 5.1.3

5.1.2.7. Implementation

5.1.2.7.1. Implementation begins after receiving required approvals is performed in accordance with the approved change plan, approved testing and validation approach, and defined risk controls and mitigations.

5.1.2.7.2. Unless permitted through the Emergency Change Process, no GxP change may be implemented before approval.

5.1.2.7.3. Ownership

5.1.2.7.3.1. The ICT Administrator is responsible for executing approved implantation activities.

5.1.2.7.3.2. The Change Owner is responsible for overseeing implementation progress and ensuring the approved plan is being adhered to.

5.1.2.7.3.3. QA maintains oversight but does not execute the approved plan.

5.1.2.7.4. Controls

5.1.2.7.4.1. Activities may only be performed within the scope of the approved change and change plan.

5.1.2.7.4.2. Without proper escalation, deviations from the plan cannot be implemented.

5.1.2.7.4.3. Evidence of implementation are gathered and retained. Evidence includes system logs, screenshots, or other objective records.

5.1.2.7.4.4. System backups and recovery measures identified in the change must be confirmed by the Change Owner and approved by QA before implementation.

5.1.2.7.5. Handling Deviations

5.1.2.7.5.1. Implementation may be paused when appropriate if deviations, failures, or unexpected outcomes occur.

5.1.2.7.5.2. Deviations must be documented in the change record.

5.1.2.7.5.3. Deviations will need to be assessed to determine the impact to GxP systems and data integrity. Other controls, planning, or escalation to QA or the CRB may be necessary.

5.1.2.7.6. Outcomes

5.1.2.7.6.1. Completion of the implementation will result in approved change activities and the generation of objective evidence that demonstrate execution according to the approved change plan.

5.1.2.7.6.2. Completion of the implementation stage does not equate to change closure or effectiveness approval.

5.1.2.8. Post-Implementation Review

5.1.2.8.1. GxP IT changes undergo a post implementation review. The scope and depth of the review will be proportionate to the impact and risk level for the change.

5.1.2.8.2. Effectiveness Check Execution

5.1.2.8.2.1. If an effectiveness check is required according to the approved change plan then effectiveness will be measured against predefined criteria. Evidence supporting effectiveness must be documented and retained.

5.1.2.8.2.2. Effectiveness checks may include targeted functional verification, a review of operational use, and confirmation of control performance.

5.1.2.8.3. Review Activities

5.1.2.8.3.1. Post-Implementation review activities may include any of the following, as applicable:

5.1.2.8.3.1.1. Confirmation that systems function as intended.

5.1.2.8.3.1.2. Review of implementation and testing evidence.

5.1.2.8.3.1.3. Verification that no unexpected issues or deviations occurred.

5.1.2.8.3.1.4. System performance or stability review.

5.1.2.8.3.2. Issues that have been identified post implementation must be documented and escalated to QA and CRB.

5.1.2.8.4. Ownership

5.1.2.8.4.1. The Change Owner is responsible for ensuring that the post-implementation review and effectiveness check have been completed.

5.1.2.8.4.2. The ICT administrator and SMEs may support execution and gathering evidence.

5.1.2.8.4.3. QA reviews the results to confirm adequacy and acceptability.

5.1.2.8.5. Outcomes

5.1.2.8.5.1. The outcome of the post-implementation review and effectiveness checks include confirmation the change achieved its desired outcome and the identification of any issues that require remediation, escalation, or additional controls.

5.1.2.8.5.2. Issues that have been unresolved must be addressed before change closure.

5.1.2.8.5.2.1. Issues may be handled in accordance with KK-QD-######, Corrective Action/Preventative Action SOP.

5.1.2.9. Emergency Change Process

5.1.2.9.1. An Emergency Change is a change that must be implemented immediately to addressed an imminent risk to system availability supporting GxP activities, data integrity, security, patient safety, or continuity of regulated operations.

5.1.2.9.2. Authorization

5.1.2.9.2.1. Emergency Changes require documented justification for the emergency classification and authorization from the E-CRB.

5.1.2.9.3. Controls

5.1.2.9.3.1. During emergency implementation, only actions that stabilize or mitigate the risk can be performed.

5.1.2.9.3.2. Implementation is limited to the minimum required scope.

5.1.2.9.3.3. Implementation activities for the emergency change must be documented to the extent feasible. Wherever standard documentation cannot be completed before implementation, it must be completed retrospectively.

5.1.2.9.4. Mandatory Retrospective Activities

5.1.2.9.4.1. Retrospective activities must be completed prior to change closure.

5.1.2.9.4.2. Risk Assessment

5.1.2.9.4.2.1. Confirm the actual impact to systems that have been validated, GxP workflows, and data integrity.

5.1.2.9.4.2.2. Identify any unintended consequences that have been introduced by the emergency change.

5.1.2.9.4.3. Validation and Testing Review

5.1.2.9.4.3.1. Confirm whether validation testing was required but deferred.

5.1.2.9.4.3.2. Execute any deferred, required validation, qualification, or testing activities.

5.1.2.9.4.4. Quality Assurance Review and Approval

5.1.2.9.4.4.1. QA reviews the justification for the emergency classification, completeness of the retrospective assessments, and the adequacy of testing and validation activities.

5.1.2.9.4.4.2. QA approval is required prior to change closure.

5.1.2.9.4.5. Escalation and Non-Compliance

5.1.2.9.4.5.1. If retrospective activities identify unacceptable residual risk or noncompliance, then the change must be escalated to the CRB and QA. Additional remediation, validation, or CAPA activities may be required.

5.1.2.9.4.6. Closure Eligibility

5.1.2.9.4.6.1. Emergency changes may proceed to closure only after all required retrospectives have been completed, identified issues have been addressed or formally managed, and all required QA approvals have been obtained.

5.1.2.10. Closure

5.1.2.10.1. Regardless of the type of change (Routine, Normal, Patch-Driven, or Emergency), closure cannot occur until all required activities are completed and approved by QA.

5.1.2.10.2. Closure Eligibility Criteria

5.1.2.10.2.1. When all of the following criteria have been met, then a change may be closed:

5.1.2.10.2.2. All approved implementation actions have been completed.

5.1.2.10.2.3. Any required testing and validation activities are completed.

5.1.2.10.2.4. Post-implementation review has been performed.

5.1.2.10.2.5. Issues, deviations, or failures have been addressed and formally managed.

5.1.2.10.2.6. Effectiveness checks, if required, have been completed.

5.1.2.10.2.7. Required evidence and documentation is complete and traceable.

5.1.2.10.2.8. For emergency changes, all mandatory retrospective activities have been completed.

5.1.2.10.3. Review and Approval

5.1.2.10.3.1. The Change Owner is responsible for confirming that the closure criteria has been met and that the change record is complete.

5.1.2.10.3.2. QA reviews the change record to confirm completely of documentation, adequacy of controls and evidence, and the acceptability of outcomes from a GxP perspective.

5.1.2.10.3.3. QA approves GxP IT changes for final closure.

5.1.2.10.4. Documentation

5.1.2.10.4.1. Documentation for closure includes completed:

5.1.2.10.4.1.1. Impact assessment

5.1.2.10.4.1.2. Risk assessment

5.1.2.10.4.1.3. Post-Implementation review

5.1.2.10.4.1.4. Effectiveness check results

5.1.2.10.4.1.5. References to affiliated deviations, incidents, or CAPAs if applicable

5.1.2.10.4.1.6. Approvals

5.1.2.10.5. Outcome

5.1.2.10.5.1. Change closure confirms that the change is incorporated into the controlled environment and that the validated state and data integrity is preserved.

5.1.2.10.5.2. A change in closure state has no outstanding GxP issues open related to the change.

5.1.2.10.5.3. Once closed, changes may not be modified without initiating a new change.

6. ASSOCIATED FORMS AND TEMPLATES:

N/A

7. REFERENCES:

7.1. AB-QD-######: Corrective Action/Preventative Action SOP

7.2. AB-QD-044574: North America Change Control Procedure

7.3. AB-QD-128633: Data Integrity Risk Assessment Process

7.4. AB-QD-144070: Sanford Site Quality Manual

8. ATTACHMENTS:

8.1. Attachment 1: IT Change Management (GxP-Related) RACI

9. VERSION HISTORY:

9.1. List the most recent version history at the top of the table below.

Version	Date of Approval	Description of Change
1.0	List document approval date or reference Vault Quality Documents (VQD) for approval date.	Change Justification: Include Document Change Control (DCC) number. Description of Change: Include brief description of changes made within the corresponding document version.

ATTACHMENT 1: IT CHANGE MANAGEMENT RACI

Change Activity	Initiator	Change Owner	System Owner	Validation Representative	ICT Admin	Business Lead	QA	CRB/E-CRB	SME
Initiation	R	A	C	I	I	C	I	I	I
Impact Assessment	I	R	C	C	C	C	A	I	C
Validation Determination	I	R	C	R	I	I	A	I	C
Change Planning	I	R	C	C	C	C	A	C	C
Approval for Implementation	I	R	C	C	I	I	A	C	I
Change Implementation	I	R	I	I	R	I	I	I	C
Deviation Handling	I	R	C	C	C	I	A	I	C
Effectiveness Check	I	R	C	C	C	I	A	I	I
Change closure	I	R	I	I	I	I	A	I	I
Emergency Change Authorization	I	R	I	C	C	I	C	A (E-CRB)	C
Retrospective Emergency Review	I	R	C	C	C	I	A	C	C
Legend	**R**: Responsible. Role performs the work. **A**: Accountable. Role confirms that the work was done and approves it. **C**: Consulted. Role advises or collaborates with the responsible role. **I**: Informed. The informed role receives task notice, news, and updates from the responsible role.								