**[System Name]**

***Vendor Assessment***



This Vendor Assessment Template (Template) is being provided by Praxis Management International, LLC (Praxis) for the "fair use" by you, the User, as that term is defined under the U.S. Copyright Laws. All other use, reproduction or re-transmission in any form or by any means, electronic or mechanical, including photocopying and recording, or by any information storage or retrieval system, without prior written permission from Praxis is prohibited. ©2008-2016 Praxis Management International, LLC. All rights reserved.

Praxis makes no representations or warranties concerning the suitability or use of, or reliance on, the Template. Any actual or implied representation or warranty that the Template does not infringe the intellectual property rights of any third party is specifically hereby void. Any special, indirect or consequential damages or any damages whatsoever resulting from the use or misuse of the Template, the loss of use, data, or profits, whether in an action of contract, negligence, or other tortious action arising out of or in connection with the Template shall be born exclusively by the User

**V.1.0**

**12 May 2016**

Contents

[1 Vendor Information 3](#_Toc431558809)

[2 Assessment Team Information 3](#_Toc431558810)

[3 Assessment Summary 4](#_Toc431558811)

[4 Assessment Questions 5](#_Toc431558812)

[A. General Information: 5](#_Toc431558813)

[B. Quality Management System (QMS) 6](#_Toc431558814)

[C. Development 9](#_Toc431558815)

[D. Verification and Validation Testing 11](#_Toc431558816)

[E. Operating Environment 13](#_Toc431558817)

[F. Defect Tracking and Corrective Actions 14](#_Toc431558818)

[G. Change and Configuration Management 15](#_Toc431558819)

[H. Archival & Disaster Recovery 16](#_Toc431558820)

[I. Security 17](#_Toc431558821)

[J. Electronic Signatures 19](#_Toc431558822)

[K. Audit Trails 20](#_Toc431558823)

[L. Service & Support 21](#_Toc431558824)

[M. Training 23](#_Toc431558825)

[5 Revision History 24](#_Toc431558826)

[6 Management Approval 24](#_Toc431558827)

# Vendor Information

|  |  |  |
| --- | --- | --- |
| VENDOR NAME |  | |
|  |  | |
| PRODUCT NAME |  | |
|  |  | |
| ASSESSMENT DATE(S) |  | |
|  |  | |
| PRIMARY CONTACT  NAME |  | |
| TITLE |  | |
| TELEPHONE |  | |
| ADDRESS |  | |
|  |  | |
| OTHER CONTACT(S)  NAME / TITLE |  |  |
| NAME / TITLE |  |  |
| NAME / TITLE |  |  |
| NAME / TITLE |  |  |

# Assessment Team Information

|  |  |  |
| --- | --- | --- |
| LEAD ASSESSOR  NAME / TITLE |  |  |
|  |  | |
| OTHER ASSESSOR(S)  NAME / TITLE |  |  |
| NAME / TITLE |  |  |
| NAME / TITLE |  |  |

# Assessment Summary

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **VENDOR RATING** | | | | | | |
|  |  |  |  |  |  |  |
|  |  | **Full Approval** |  | Unrestricted approval is granted to the vendor. | | |
|  |  |  |  |  |  |  |
|  |  | **Restricted Approval** |  | Limited approval is granted to the vendor. Limitations, reasons for restrictions, and conditions for removal of restrictions are documented in the Summary Statements, below. | | |
|  |  |  |  |  |  |  |
|  |  | **Not Approved** |  | Limited approval is granted to the vendor. Reasons for disapproval are documented in the Summary Statements, below. | | |

|  |
| --- |
| **SUMMARY STATEMENTS** |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |
|  |

**Question Rating System**

|  |  |  |
| --- | --- | --- |
| Rating | Definition | Interpretation |
| 3 | Excellent | Exceeds minimum requirements |
| 2 | Satisfactory | Meets minimum requirements |
| 1 | Unsatisfactory | Does not meet minimum requirements |
| N/A | Not applicable | Question does not apply to the vendor or product |

# Assessment Questions

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| General Information: |  |  | |
| 1. Background:  * How long has the vendor been in business? * What industries are well represented in the vendor’s customer base? * What is the installed base of the product of interest? |  |  |
| 1. Financials (optional):  * Are financial statements for the last 2 years available for review? * Is an independent financial rating available? |  |  |
| 1. Management:  * What are the backgrounds of key members of management? * Do key management personnel have compliance, regulatory and/or validation experience? * Do any debarred individuals work for the company? If so, what are their roles? |  |  |
| 1. Certification  * Does vendor have ISO, Malcolm Baldridge or other certification? If yes, request copy. |  |  |
| 1. Outlook  * Do the vendor’s strategy, business outlook, and organizational structure suggest a long-term commitment to the product and industry? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Quality Management System (QMS) |  |  |
| 1. Quality Assurance Organization:   * Obtain organization chart. * Is there an independent QA organization? * Has the QA organization’s responsibilities and authority been formalized? * What is the QA organization’s role? * In design * In development * In testing * In product release * In auditing |  |  |
| 2. QMS SOPs:   * Do Quality Management System SOPs exist? * Are QMS SOPs under change control? * Is there a revision history for QMS SOPs? * Is there a system for periodic management review of these documents? * Are the QMS SOPs adequate? * How well does the vendor conform to the QMS SOPs? Explain. |  |  |
| 3. Quality Assurance Plan (QAP):   * Is there a software Quality Assurance Plan? * Does the software QAP follow an industry standard, such as ANSI/IEEE or equivalent? * Is the software QAP adequate? Does it include:   + Formalized development life cycle   + Risk assessment and mitigation process   + Clear responsibilities   + Inspection and testing methodology   + Appropriate documentation requirements? |  |  |
| 4. Validation Master Plan (VMP):   * Is there a Validation Master Plan that includes computer systems? * Is the system VMP adequate? Does it include:   + Overview of the validation process, change management process, periodic validation review process   + Risk management approach (Annex 11(1))   + Standard acceptance criteria   + Validation roles and responsibilities   + Inventory of validated systems with the validation status, risk level, and next planned validation activity for each? (Annex 11(4.3)) |  |  |
| 5. Periodic Validation Review:   * Is there a Periodic Validation Review procedure and schedule? (Annex 11(11)) * Is the Periodic Validation Review frequency risk-based? * Is the Periodic Validation Review procedure adequate? Does it include review of:   + Application and infrastructure changes and revalidation   + Validation documentation   + Incidents and reported defects   + Current use vs. validated intended use   + Regulation changes |  |  |
| 6. Responsibilities:   * Are individual and departmental responsibilities documented for: * Software development * Software testing * Product release? * Is the Quality Assurance organization’s role clearly separated from the Development, Support, Sales, and Marketing organizations? |  |  |
| 7. Releases:   * Is there an overseeing function, such as a product steering committee or software management board, to review and approve product releases? * Does the Quality Assurance organization have the authorization to prevent software/system release? |  |  |
| 8. QA assessments:   * Are there adequate, independent quality assurance assessments throughout the software development process? * Are there documented quality assurance reviews and approvals of test data? |  |  |
| 9. Document retention and versioning:   * What is the retention time period for all system related documentation? * User requirements specifications * Functional requirements specifications * Design documents * Maintenance records * Testing records * Training records * Are file locations, retention times, and/or destruction criteria adequately defined? * Is system related documentation under change control and protected from unauthorized modification as required by 21 CFR Part 11.10(k)? * Is system related documentation versioned and are versions retained to allow for a time-sequenced review of product development and modification as required by 21 CFR Part 11.10(k)? |  |  |
| 10. Internal audits:   * Does the vendor require that internal audits be conducted? * Are internal audit results recorded and reviewed by management? * Are audits followed up with timely corrective actions? |  |  |
| 11. Continuous improvement:   * Are metrics used to measure the performance and effectiveness of the quality management system? * Does the vendor have a continuous quality improvement program? |  |  |
| 12. Suppliers:   * Is there an adequate supplier audit program? (Annex 11(3) and (4.5)) * How are suppliers qualified? Is qualification method based on level of risk? * Are there adequate controls over the transfer of supplier hardware and software into the organization’s operations? What is the process? |  |  |
| 11. Inspections:   * Has the vendor been inspected by FDA or other international regulatory authority? If yes, provide dates. * Are copies of inspection reports available for review? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Development |  |  |
| 1. Technical resources:   * Does the vendor have its own development staff? If so, how many? * What is the percentage of contract developers vs. Vendor employed developers? * What is the turnover rate? * What are the technical qualifications? * Do technical resources have FDA regulatory compliance experience? * If custom coding is required, can resumes, job description, and training records be made accessible with an appropriate non-disclosure agreement? |  |  |
| 2. Accountability:   * Are there records in place that can easily identify which programmer created or revised each portion of the source code? |  |  |
| 3. Standards:   * Do formal coding standards and/or guidelines exist? If yes, do they contain requirements for: * Entity naming conventions * Revision level notations * Program descriptions * Data flow diagrams * Structured coding? * Do formal user interface standards and/or guidelines exist? * Do formal documentation standards and/or exist? If yes, review examples. * Are all standards under change control? |  |  |
| 4. Software development methodology:   * Is a formal methodology used for software development? If yes, identify. * What quality assurance steps are included in the methodology? |  |  |
| 5. Risk assessment:   * Is a formal methodology used for software risk assessment? If yes, identify. * Does the methodology include the evaluation of risks based on potential severity of impact to patients, regulated products, and data integrity? (Annex 11(1)) * Does the methodology include the evaluation of risks based on system complexity and novelty? |  |  |
| 6. Risk mitigation   * How does the Risk Assessment impact SDLC activities? (Annex 11(1))   + Design of features   + Design Reviews   + Code Reviews   + Documentation level of detail |  |  |
| 7. Specifications and Design:   * Are User Requirements documented and approved prior to system development or modification? Are system users included in defining these requirements? (Annex 11(4.4)) * Are Functional Requirements documented and approved prior to system development or modification? Are functional requirements adequately detailed to enable thorough testing? * Are System Designs documented and approved prior to system development? Are designs adequately detailed to prevent ad hoc decisions from developers? * Are requirements and design documents updated when system changes are made? |  |  |
| 8. Development plans:   * Are software development plans prepared and approved? * Are the development plans adequate? Do they include:   + Software definition and description   + Risk mitigation and control   + Resource identification and responsibilities   + Development schedules? |  |  |
| 1. Design Reviews:  * Are design reviews performed and documented? * If yes, do design reviews include review of design vs. requirements, standards, and defined risks? |  |  |
| 10. Code Reviews   * Are code reviews performed and documented? |  |  |
| 11. Traceablity:   * Are there traceability matrices between?   + Risks and specifications (Annex 11(4.4))   + Specification and designs (Annex 11(4.4))   + Designs and programs |  |  |
| 12. Tools:   * Are any software tools used to assist with program development? If yes, identify. * Dependent on risk level, have the tools been validated or qualified? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Verification and Validation Testing |  |  |
| 1. 21 CFR Part 11 requirements:   * + Has the product been validated as required by 21 CFR Part 11.10(a)?   + Does the validation provide evidence of the system’s ability to generate accurate and complete copies of electronic records in both human readable and electronic formats, as required by 21 CFR Part 11.10(b)? |  |  |
| 2. Procedures:   * Are there adequate written procedures for validating and testing? * Are there adequate written procedures for recording, storing, and auditing test results? |  |  |
| 3. Validation Plan   * Are Validation Plans prepared and approved? * Do Validation Plans document: * Validation approach and deliverables * Validation roles and responsibilities * Risk mitigation (Annex 11(1)) * Procedures for validation documentation, test failures * Procedures and training required to ensure intended use * Acceptance criteria? |  |  |
| 4. Test plans/protocols:   * Are test plans/protocols prepared and approved? (Annex 11(4.7)) * Do test plans/protocols document: * Identification of entities to be tested * Type of testing to be performed * Testing schedules * Testing responsibilities * Documentation requirements * Acceptance criteria * Test incident/failure handling * Error resolution? * Describe test approach. * Do testing techniques include normal case (positive), invalid case (negative), repeatability, performance, volume/load, and structural testing? * Does test data mimic valid, invalid, boundary values, and error conditions? * Describe data choices. * Describe test scripts. |  |  |
| 5. Risk mitigation   * How does the Risk Assessment impact Validation activities? (Annex 11(4.1)) * How does the Risk Assessment impact testing activities? * Are validation activities and the degree of testing based on the level of risk (e.g., criticality to patient, complexity of novelty of technology) (Annex 11(1)) |  |  |
| 6. Traceability:   * Can tests and acceptance criteria be mapped to the specifications? |  |  |
| 7. Regression testing:   * Under what circumstances is regression testing done? * What tools are used? Dependent upon risk, are regression testing tools validated or qualified? |  |  |
| 8. Retention:   * How long are test plans/protocols retained? * How long are test results retained? |  |  |
| 9. Tools:   * Are software tools used to assist with testing? If yes, identify. * Are software tools used to assist with resolving software bugs? If yes, identify. * Dependent on risk level, have the tools been validated or qualified? (Annex 11 4.7)) |  |  |
| 10. Validation support services:   * Is the vendor able to supply test protocols to the customer? * Is the vendor able to assist in the customer’s site validation effort? If yes, describe assistance. |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Operating Environment |  |  |
| 1. Design and Qualification:   * Is the operating environment documented in the System Design? * Is there documentation that the operating environment has been established according to the System Design, e.g., via an Installation Qualification? |  |  |
| 2. Change Management:   * Are changes to the operating environment documented and authorized? * Are changes to the operating environment assessed for the impact and risk that the change might pose to the system? * Is appropriate regression testing performed? * Is the System Design updated when operating environment changes are made? * Is there documentation that changes to the operating environment have been made according to the updated System Design, e.g., via an Installation Qualification? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Defect Tracking and Corrective Actions |  |  |
| 1. Defect tracking:   * Are records maintained of all known problems for each revision? * Are errors, bugs, and defects assessed and categorized by severity, urgency, and priority? * Does tracking include data errors, user errors, outages, and other issues not caused by system functionality? (Annex 11 (13)) * Does documentation include changes that were made to correct problems? * Does the vendor have an effective program for resolving documented defects? |  |  |
| 2. Correction procedures:   * What are the corrective action procedures for resolving software problems discovered in the testing process? * What are the corrective action procedures for resolving software problems discovered after product release? |  |  |
| 3. Trending and prevention:   * Are defects trended and assessed to identify systemic problems? * What are the preventative action procedures for critical and systemic problems? * Do these procedures include root cause analysis for critical incidents? (Annex 11(13)) * Are preventative actions tracked and managed to timely completion? Are actions effective? |  |  |
| 4. Defect Resolution Testing:   * Is adequate regression testing performed and documented after performing corrective action to resolve defects? |  |  |
| 5. New releases:   * How are the solutions to reported defects integrated into new releases? Illustrate by sampling. |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Change and Configuration Management |  |  |
| 1. Change Management:   * Are changes to the system documented, authorized, and performed according to a defined procedure? (Annex 11(10)) * Are changes assessed for the impact and risk that the changes might impose on existing system functionality? * Are the system’s Requirements and Design documents updated when changes are made? * Is there documentation that changes to the system have been made according to the updated System Design, e.g., via an Installation Qualification? |  |  |
| 2. Revalidation:   * Does the vendor adequately evaluate software changes to determine the extent of revalidation required? * Is appropriate regression testing performed? |  |  |
| 3. Version control:   * Does the vendor have an adequate software version control program? * Can prior versions of code be recreated? |  |  |
| 4. Source code protection:   * How are source code, programs, and configuration settings managed and protected? * Who has access? * Describe how the source code for a given release is controlled. |  |  |
| 5. Tools:   * Is a configuration management tool used? If yes, identify. * How is the tool administered? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Archival & Disaster Recovery |  |  |
| 1. Source code retention:   * What is the backup and storage schedule for source code? * What off-site arrangements have been made? * Is source code archived? * What is the archival process? * How long is the archive retained? * Who has access to the archive? * What arrangements are available for code to be held in escrow in case of business failure? |  |  |
| 2. Executable and Configuration retention.   * How are executable objects and application configurations protected from loss? * What is the backup and storage schedule for executable objects and application configurations? * What off-site arrangements have been made? * Are objects and configurations adequately to allow appropriate recovery times? |  |  |
| 3. Source code escrow:   * What arrangements are available for code to be held in escrow in case of business failure? |  |  |
| 4. Data and Record retention:   * How are data and electronic records protected from loss? * What is the backup and storage schedule for data and electronic records? Annex 11(7.1) * What off-site arrangements have been made? * Has the back-up process been validated? Annex 11(7.2) * Are recorded periodically archived? * Is the accuracy of the back-ups and archives periodically checked? Annex 11(7.2) and (17) * Are records stored adequately to allow appropriate recovery times? * Are record retention practices adequate to enable accurate and ready retrieval throughout the records retention period, as required by 21 CFR 11.10(c) and Annex 11(7.1)? |  |  |
| 5. Disaster recovery:   * Is there a disaster recovery plan? * Has it been tested? |  |  |
| 6. Disaster contingency:   * Are there disaster contingency or business continuity procedures for critical systems? Annex 11(16) * Have the procedures been documented and tested? Annex 11(16) |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Security |  |  |
| 1. Source code & executable protection:   * Is there an authorization list of personnel who have access to source code and executables? * How is access authorized? * Is there and adequate security system to prevent unauthorized modification of source code, builds, and distribution copies of software? * What are the security measures? |  |  |
| 2. Physical security:   * Are the facilities (e.g., computer rooms, data centers) adequately secured against unauthorized entry? (Annex 11(12.1)) * Is there a documented authorization list? * How is access authorized? |  |  |
| 3. Electronic records and signature security requirements:   * Does the system provide logical security that requires unique user identification as required by 21 CFR Part 11.100(a) and 200(a) and Annex 11(12.1)? * Does user identification require 2 components, e.g., user ID and password, a adequately complex passwords to ensure use by only the genuine owner, as required by 21 CFR Part 11.200(a) and 300(a)? * When an individual executes a series of signings during a single, continuous period of controlled system access, does the first signing require both User ID and password? And, does any subsequent signings require entry of at least the password, as required by 21 CFR 11.200(a)? * Does the password require periodic revision as required by 21 CFR Part 11.300(b)? * Does the system have the capability of limiting system access to authorized individuals as required by 21 CFR Part 11.10(d)? * Does the system log out users after a period of inactivity? Reference 21 CFR Part 11.10(d) * Does the system have the capability of limiting access to authorized individuals for viewing, creating, altering, and signing electronic records as required by 21 CFR Part 11.10(g)? * Does the system provide transaction safeguards to report and prevent unauthorized attempts to enter the system as required by 21 CFR Part 11.300(d)? |  |  |
| 4. Specifications and Testing:   * Do the system specifications adequately communicate security measures required by 21 CFR Part 11? * Does testing demonstrate the fulfilment of the security specifications for 21 CFR Part 11? |  |  |
| 5. User Access Controls   * Is user access granted, changed, and deleted according to a defined procedure? (Annex 11(12.3))? * Does the procedure include verification of training? * Does the procedure include creation and retention of records regarding user access? (Annex 11(12.3))? |  |  |
| 6. Identity Verification:   * When electronic signatures are in use, does the organization verify the identity of the individual prior to issuing an electronic signature, as required by 21 CFR Part 11.100(b)? |  |  |
| 7. Device checks:   * Is the product capable of verifying the validity of source data inputs as required by 21 CFR Part 11.10(h)? |  |  |
| 6. Open system requirements:   * For open systems, does the product have controls designed to ensure the authenticity, integrity, and, as appropriate, the confidentiality of electronic records from the point of their creation to the point of their receipt as required by 21 CFR Part 11.30? * Do these controls include document encryption and use of digital signatures? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Electronic Signatures |  |  |
| 1. Electronic signature requirements:   * Does the product link the electronic signature to the electronic record in a way that ensures that the signatures cannot be excised, copied, or otherwise transferred to another record, as required by 21 CFR Part 11.70 and Annex 11(14b)? |  |  |
| 2. Electronic signature review:   * Does the product display and print the electronic signature in human readable format, as required by 21 CFR Part 11.50(b)? * Does the display include the printed name of the signer, the date and time of the signature, and the meaning of the signature, as required by 21 CFR Part 11.50(a) and Annex 11(14c)? |  |  |
| 3. Specifications and Testing:   * Do the system specifications adequately communicate electronic signature requirements defined by 21 CFR Part 11? * Does testing demonstrate the fulfilment of the electronic signature specifications for 21 CFR Part 11? |  |  |
| 4. FDA Certification:   * If the vendor is using electronic signatures for FDA-regulated activities, has the organization certified to the FDA the electronic signatures are in use and are intended to be the legally binding equivalent of handwritten signatures? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Audit Trails |  |  |
| 1. Audit Trail features:   * Does the system generate an audit trail of the creation, modification, and deletion of all GxP records, as required by 21 CFR Part 11.10(e) and Annex 11(9)? * Is the audit trail generated automatically and independent of user intervention, as required by 21 CFR Part 11.10(e)? * Does the audit trail contain all versions of the electronic record, as required by 21 CFR Part 11.10(e)? * Is the audit trail secured from alterations or deletions, as required by 21 CFR Part 11.10(e)? * Does the audit trail capture the reason for electronic record revision or deletion? |  |  |
| 2. Audit Trail retention:   * Is the product capable of retaining the audit trail for the same duration and the subject electronic record as required by 21 CFR Part 11.10(e)? |  |  |
| 3. Audit Trail review:   * Are systems capable of displaying or printing the audit trail so that is can be reviewed or provided to a regulatory agency for inspection, as required by 21 CFR Part 11.10(e) and Annex 11(9)? * Are audit trails regularly reviewed by company personnel? (Annex 11(9)) * Do records supporting batch release clearly indicate changes data when printed? (Annex 11(8.2)) |  |  |
| 4. Specifications and Testing:   * Do the system specifications adequately communicate audit trail requirements defined by 21 CFR Part 11? * Does testing demonstrate the fulfilment of the audit trail specifications for 21 CFR Part 11? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Service & Support |  |  |
| 1. Maintenance and support agreement:   * Does the vendor utilize a maintenance/support agreement? * Does the agreement include clear statements of the responsibilities of the vendor and the customer? E.g., issue resolution, backup/recovery, system and data administration, periodic maintenance and performance tuning * Does the agreement include service level targets such as processes for monitoring, reporting, and review for adherence to service targets? * How long are software product elements maintained and supported? |  |  |
| 2. Performance monitoring:   * Does the vendor utilize a performance monitoring plan for the product? * Does the plan include responsibilities, performance targets and thresholds for escalation, monitoring frequency and approach, reporting and review mechanisms? |  |  |
| 3. Help desk:   * Is the vendor’s help desk support function for software and hardware adequate? * What is the availability of the help desk? * How are calls logged? * Are metrics of logged calls tracked? |  |  |
| 4. Notification:   * Are there adequate practices and procedures to notify customers when a critical defect is discovered? * What is the time frame of notification? |  |  |
| 5. New releases:   * Is there an adequate product release and distribution system? * What is the frequency of major releases? * Does the documentation for new releases of the product provide enough information to allow the customer to determine the impact of every change in the release? |  |  |
| 6. Prior releases:   * Are prior releases adequately supported? * How long are prior releases supported? * Must the customer always upgrade to the latest release? |  |  |
| 7. Technical manual:   * Is a technical manual provided with the software? * Is it clear and understandable? * Are updates to the manual provided to the customer with new releases and product updates? |  |  |
| 8. User manual:   * Is a user manual provided with the software? * Is it clear and understandable? * Are updates to the manual provided to the customer with new releases and product updates? |  |  |
| 9. Customization/enhancements:   * What is the procedure for requesting custom coding that is not standard implementation? * How well does the vendor act upon requests for product enhancements? |  |  |
| 10. Online help:   * Is there an on-line help facility within the application? |  |  |
| 11. User groups:   * Are there user group meetings? * If yes, how frequently? * Who coordinates the meetings? * Who participates? |  |  |

| Item / Question | Rating | Describe Results |
| --- | --- | --- |
| Training |  |  |
| 1. Training program:   * Is there an adequate training program for engineers, operators, programmers, testers, help desk & support staff, as required by 21 CFR 11.10(i) and Annex 11(2)? * Is there an adequate training program for system users, as required by 21 CFR 11.10(i) and Annex 11(2)? * Are sub-contractors included in training program? * Does training include ongoing technical training? * Where applicable, does training include cGMP, cGLP, cGCP, 21 CFR Part 11? * When electronic signatures are in use, is there training on the written policies that hold individuals accountable and responsible for actions initiated under their electronic signatures, as required by 21 CFR 11.10(j) and Annex 11(14a)? * Does training include the organization’s QMS? * Is a training matrix available for review? |  |  |
| 2. Training records:   * Are there employee and contractor training records for all personnel involved in developing, using, and supporting systems? * Do the records demonstrate adequate compliance with the training program? * Is there documentation available that demonstrates the qualifications of all programmers who have worked on the product? |  |  |

# Revision History

|  |  |  |  |
| --- | --- | --- | --- |
| **Document Version Number** | **Document Revision Date** | **Revisions Made By:** | **Revision Summary**  *(Reference section[s] changed)* |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

# Management Approval

Signatures indicate approval of this Vendor Assessment.

| Document Approvals: | | | |
| --- | --- | --- | --- |
| Function | Name | Signature | Date |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**\*\*\*END OF DOCUMENT\*\*\***