--- GAMP5 - Validated IT Systems Info.docx ---  
GAMP 5 – Validated IT Systems  
  
  
Purpose  
The purpose of this Guide is to provide a cost-effective framework of good practice to ensure that computerized  
systems are effective and of high quality, fit for intended use, and compliant with applicable regulations. The  
framework aims to safeguard patient safety, product quality, and data integrity while also delivering business benefit.  
This Guide also provides suppliers to the life-science industry with guidance on the development and maintenance of  
systems by following good practice.  
Patient safety is affected by the integrity of critical records, data, and decisions, as well as those aspects affecting  
physical attributes of the product. The phrase “patient safety, product quality, and data integrity” is used throughout  
this Guide to underline this point.  
This Guide is intended for use by regulated companies, suppliers, and regulators. Suppliers include providers  
of software, hardware, equipment, system integration services, IT service providers, and IT support services, both  
internal and external to the regulated company.  
  
  
Quality Risk Management  
Chapter 3 introduced the concept of QRM as part of the life cycle approach. This section gives an overview of the  
QRM process and Appendix M3 provides more detail.  
This section is primarily aimed at new computerized systems. It does not imply that formal risk assessments are  
required for all existing systems. The extent of risk management required for existing systems, including the need for  
formal risk assessments, should be considered as part of periodic review.  
This section focuses on software products and custom applications rather than on infrastructure.  
5.1 Overview  
QRM is a systematic process for the assessment, control, communication, and review of risks. It is an iterative  
process used throughout the computerized system life cycle from concept to retirement.  
Figure 5.1 indicates key areas for risk management and the benefits of the approach.  
Figure 5.1: Overview and Benefits of Risk Management  
  
For a given organization, a framework for making risk-management decisions should be defined to ensure  
consistency of application across systems and business functions. Terminology should be agreed upon, particularly  
regarding definitions and metrics for key risk factors.  
Such a framework is most effectively implemented when it is incorporated into the overall QMS and is fully integrated  
with the system life cycle.  
  
Science-Based Quality Risk Management  
Determining the risks posed by a computerized system requires a common and shared understanding of:  
• Impact of the computerized system on patient safety, product quality, and data integrity  
• Supported business processes  
• CQAs for systems that monitor or control CPPs  
• User requirements  
• Regulatory requirements  
• Project approach (contracts, methods, timelines)  
• System components and architecture  
• System functions  
• Supplier capability  
The organization also should consider other applicable risks, such as Health, Safety, and Environment (HSE).  
Managing the risks may be achieved by:  
• Elimination by design  
• Reduction to an acceptable level  
• Verification to demonstrate that risks are managed to an acceptable level  
It is desirable to eliminate risk, if possible, by modifying processes or system design. Design reviews can play a key  
role in eliminating risk by design.  
Risks that cannot be eliminated by design should be reduced to an acceptable level by controls or manual  
procedures. Risk reduction includes applying controls to lower the severity, decrease probability, or increase  
detectability.  
A systematic approach should be defined to verify that the risk associated with a system has been managed to an  
acceptable level. The overall extent of verification and the level of detail of documentation should be based on the risk  
to patient safety, product quality, and data integrity, and take into account the complexity and novelty of the system.  
The information needed to perform risk assessments may become available, and should be considered, at different  
stages in the life cycle. For example, the high-level risks associated with a business process need to be understood  
before the risks associated with specific functions of computerized systems can be assessed.3  
The criticality of a business process is independent of whether it is manually processed, semi-automated, or fully  
automated. Systems that support critical processes include those that:  
• Generate, manipulate, or control data supporting regulatory safety and efficacy submissions  
• Control critical parameters and data in pre-clinical, clinical, development, and manufacturing  
• Control or provide data or information for product release  
• Control data or information required in case of product recall  
• Control adverse event or complaint recording or reporting  
• Support pharmacovigilance  
  
Quality Risk Management Process  
The ICH Q9 [14] describes a systematic approach to QRM intended for general application within the pharmaceutical  
industry. It defines the following two primary principles of QRM:  
• “The evaluation of the risk to quality should be based on scientific knowledge and ultimately link to the  
protection of the patient; and  
• The level of effort, formality and documentation of the quality risk-management process should be  
commensurate with the level of risk.”  
In the context of computerized systems, scientific knowledge is based upon the system specifications and the  
business process being supported.  
This Guide uses the following key terms from ICH Q9 [14]:  
“Harm: Damage to health, including the damage that can occur from loss of product quality or availability.”  
“Hazard: The potential source of harm.”  
“Risk: The combination of the probability of occurrence of harm and the severity of that harm.”  
“Severity: A measure of the possible consequences of a hazard.”  
This Guide applies the general principles of ICH Q9 [14] to describe a five-step process for risk management as an  
integral part of achieving and maintaining system compliance. For simple or low-risk systems, some of these steps  
may be combined. See Appendix M3 for further details on the QRM process.  
This process is focused on managing risks during the project phase. Risk management should also be used  
appropriately both within specific activities and during the operational phase. Examples include:  
1. Determining the need for supplier audit as part of supplier assessment  
2. Determining the rigor and extent of testing  
3. Determining corrective actions arising from test failures  
4. Determining the impact of proposed changes as part of change management  
5. Determining the frequency of periodic reviews  
Application of risk management to the above activities is covered in the appropriate sections of this Guide.  
Organizations may have established risk-management processes, including the use of methods such as those listed  
in Appendix M3. While this Guide describes one suggested approach, it does not intend or imply that these existing  
methods should be discarded, rather that they continue to be used, as appropriate, within the context of an overall  
QRM framework consistent with ICH Q9 [14].  
Process Risk Assessment  
Some records and data may reside on more than one system during their life cycle, and QRM activities should start  
at the business process level, at a level higher than individual systems. A process risk assessment (also known as  
business process risk assessment) is a non-system-specific high-level assessment of the business process or data  
flow, which may occur before system-specific QRM activities. An equivalent risk assessment from a data flow (rather  
than business process flow) perspective may be performed, using the same approaches and techniques, and with the  
same benefits.  
The process risk assessment is aimed at identifying key high-level risks to patient safety, product quality, and data  
integrity, and identifying the required controls to manage those risks. Typically, at this stage no assumptions are made  
about the nature or exact functionality and design of the computerized system(s) that will support the process.  
The process risk assessment provides valuable input to subsequent QRM activities. Typical inputs to the process risk  
assessment include:  
• Defined business process scope  
• Process descriptions and/or diagrams  
• Identified regulatory requirements for the proposed process scope  
• Identified company quality requirements  
  
Step 1 – Perform Initial Risk Assessment and Determine System Impact  
An initial risk assessment should be performed based on an understanding of business processes and business  
risk assessments, user requirements, regulatory requirements, and known functional areas. A system cannot have a  
higher impact than the business process it supports. Any relevant previous assessments may provide useful input,  
and these should not be repeated unnecessarily.  
The results of this initial risk assessment should include a decision on whether the system is GxP regulated (i.e., GxP  
assessment). It also should include an overall assessment of system impact. The scope and objectives of any further  
risk assessments should be defined.  
Based on this initial risk assessment and resulting system impact, it may not be necessary to perform the subsequent  
steps of the process, as the level of risk may already be at an acceptable level.  
The specific level of effort, formality, and documentation of any subsequent steps should be determined based on  
level of risk and system impact. See Appendix M3 for further details.  
If relevant, regulated electronic records and signatures should be identified. Again, existing assessments may provide  
useful input and should not be repeated. A detailed approach and specific guidance is provided in the ISPE GAMP  
Guide: Records and Data Integrity [35]  
Step 2 – Identify Functions with Impact on Patient Safety, Product Quality, and Data Integrity  
Functions that have an impact on patient safety, product quality, and data integrity should be identified by building  
on information gathered during Step 1, referring to relevant specifications, and considering project approach, system  
architecture, and categorization of system components. Individual functions cannot have a higher impact that the  
system as a whole.  
Step 3 – Perform Functional Risk Assessments and Identify Controls  
Functions identified during Step 2 should be assessed by considering possible hazards, and how the potential harm  
arising from these hazards may be controlled.  
It may be necessary to perform a more detailed assessment that analyzes further the severity of harm, likelihood of  
occurrence, and probability of detection. See Appendix M3 – Section 11.5 for an example detailed assessment process.  
  
The judgment as to whether to perform a detailed assessment for specific functions should be dealt with on a case-  
by-case basis and the criteria can vary widely. The criteria to be considered include:  
  
• Criticality of the supported process  
• Specific impact of the function within the process  
• Nature of the system (e.g., complexity and novelty)  
Appropriate controls should be identified based on the assessment. A range of options is available to provide the  
required control depending on the identified risk. These include, but are not limited to:  
• Modification of process design  
• Modification of system design  
• Application of external procedures  
• Increasing the detail or formality of specifications  
• Increasing the number and level of detail of design reviews  
• Increasing the extent or rigor of verification activities  
Where possible, elimination of risk by design is the preferred approach.  
Step 4 – Implement and Verify Appropriate Controls  
The control measures identified in Step 3 should be implemented and verified to ensure that they have been  
successfully implemented. Controls should be traceable to the relevant identified risks.  
The verification activity should demonstrate that the controls are effective in performing the required risk reduction.  
The effort, formality, and documentation of the verification activity should be commensurate with the level of risk.  
Step 5 – Review Risks and Monitor Controls  
During periodic review of systems, or at other defined points, an organization should review the risks. The review  
should verify that controls are still effective, with corrective action taken under change management if deficiencies are  
found. The organization also should consider whether:  
• Previously unrecognized hazards are present  
• Previously identified hazards are no longer applicable  
• The estimated risk associated with a hazard is no longer acceptable  
• The original assessment is otherwise invalidated (e.g., following changes to applicable regulations or change of  
system use)  
Where necessary, the results of the evaluation should be fed back into the risk-management process. If there is a  
potential that the residual risk or its acceptability has changed, the impact on previously implemented risk control  
measures should be considered, and the results of the evaluation documented. It should be noted that some changes  
may justify relaxation of existing controls.  
The frequency and extent of any periodic review should be based on the level of risk and should consider previous  
findings and operational history.  
  
--- Guidance-Computer-Software-Assurance.docx ---  
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
Computer Software Assurance for Production and Quality System Software   
\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Draft Guidance for Industry and Food and Drug Administration Staff   
DRAFT GUIDANCE   
This draft guidance document is being distributed for comment purposes only.   
Document issued on September 13, 2022.   
You should submit comments and suggestions regarding this draft document within 60 days of publication in the Federal Register of the notice announcing the availability of the draft guidance. Submit electronic comments to https://www.regulations.gov. Submit written comments to the Dockets Management Staff, Food and Drug Administration, 5630 Fishers Lane, Room 1061, (HFA-305), Rockville, MD 20852. Identify all comments with the docket number listed in the notice of availability that publishes in the Federal Register.   
For questions about this document regarding CDRH-regulated devices, contact the Compliance and Quality Staff at 301-796-5577 or by email at CaseforQuality@fda.hhs.gov. For questions about this document regarding CBER-regulated devices, contact the Office of Communication, Outreach, and Development (OCOD) at 1-800-835-4709 or 240-402-8010, or by email at ocod@fda.hhs.gov.   
U.S. Department of Health and Human Services   
Food and Drug Administration   
Center for Devices and Radiological Health   
Center for Biologics Evaluation and Research   
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
Preface   
Additional Copies   
CDRH   
Additional copies are available from the Internet. You may also send an email request to CDRH Guidance@fda.hhs.gov to receive a copy of the guidance. Please include the document number 17045 and complete title of the guidance in the request.   
CBER   
Additional copies are available from the Center for Biologics Evaluation and Research (CBER), Office of Communication, Outreach, and Development (OCOD), 10903 New Hampshire Ave., Bldg. 71, Room 3128, Silver Spring, MD 20993-0002, or by calling 1-800-835-4709 or 240-402- 8010, by email, ocod@fda.hhs.gov or from the Internet at https://www.fda.gov/vaccines-blood biologics/guidance-compliance-regulatory-information-biologics/biologics-guidances.  
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
Table of Contents   
I. Introduction..........................................................................................................................................................4 II. Background ..........................................................................................................................................................5 III. Scope....................................................................................................................................................................6 IV. Computer Software Assurance.............................................................................................................................6 V. Computer Software Assurance Risk Framework .................................................................................................7   
Identifying the Intended Use ........................................................................................................................7 Determining the Risk-Based Approach........................................................................................................9 Determining the Appropriate Assurance Activities ...................................................................................13 Establishing the Appropriate Record .........................................................................................................16   
Appendix A. Examples................................................................................................................................................20 Example 1: Nonconformance Management System...............................................................................................20 Example 2: Learning Management System (LMS) ................................................................................................23 Example 3: Business Intelligence Applications......................................................................................................24  
Contains Nonbinding Recommendations Draft – Not for Implementation   
1 Computer Software Assurance for 2 Production and Quality System 3 Software   
4 \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 5 Draft Guidance for Industry and 6 Food and Drug Administration Staff 7   
  
  
8   
9   
10   
11   
12   
13   
14   
I. Introduction1   
15   
16 FDA is issuing this draft guidance to provide recommendations on computer software assurance 17 for computers and automated data processing systems used as part of medical device production 18 or the quality system. This draft guidance is intended to:   
19   
20 ∙ Describe “computer software assurance” as a risk-based approach to establish confidence 21 in the automation used for production or quality systems, and identify where additional 22 rigor may be appropriate; and   
23   
24 ∙ Describe various methods and testing activities that may be applied to establish computer 25 software assurance and provide objective evidence to fulfill regulatory requirements, 26 such as computer software validation requirements in 21 CFR part 820 (Part 820). 27   
28 When final, this guidance will supplement FDA’s guidance, “General Principles of Software Validation” (“Software Validation guidance”)2   
29 except this guidance will supersede Section 6 30 (“Validation of Automated Process Equipment and Quality System Software”) of the Software 31 Validation guidance.   
32   
1 This guidance has been prepared by the Center for Devices and Radiological Health (CDRH) and the Center for Biologics Evaluation and Research (CBER) in consultation with the Center for Drug Evaluation and Research (CDER), Office of Combination Products (OCP), and Office of Regulatory Affairs (ORA).   
2 Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/general-principles software-validation.   
4   
Contains Nonbinding Recommendations Draft – Not for Implementation   
33 For the current edition of the FDA-recognized consensus standard referenced in this document,   
see the FDA Recognized Consensus Standards Database.3   
34   
35   
36 In general, FDA’s guidance documents do not establish legally enforceable responsibilities. 37 Instead, guidances describe the Agency’s current thinking on a topic and should be viewed only 38 as recommendations, unless specific regulatory or statutory requirements are cited. The use of 39 the word should in Agency guidances means that something is suggested or recommended, but 40 not required.   
41   
42 II. Background   
43 FDA envisions a future state where the medical device ecosystem is inherently focused on device 44 features and manufacturing practices that promote product quality and patient safety. FDA has 45 sought to identify and promote successful manufacturing practices and help device 46 manufacturers raise their manufacturing quality level. In doing so, one goal is to help 47 manufacturers produce high-quality medical devices that align with the laws and regulations 48 implemented by FDA. Compliance with the Quality System regulation, Part 820, is required for 49 manufacturers of finished medical devices to the extent they engage in operations to which Part 50 820 applies. The Quality System regulation includes requirements for medical device 51 manufacturers to develop, conduct, control, and monitor production processes to ensure that a 52 device conforms to its specifications (21 CFR 820.70, Production and Process Controls), 53 including requirements for manufacturers to validate computer software used as part of production or the quality system for its intended use (see 21 CFR 820.70(i)).4   
54 Recommending 55 best practices should promote product quality and patient safety, and correlate to higher-quality 56 outcomes. This draft guidance addresses practices relating to computers and automated data 57 processing systems used as part of production or the quality system.   
58   
59 In recent years, advances in manufacturing technologies, including the adoption of automation, 60 robotics, simulation, and other digital capabilities, have allowed manufacturers to reduce sources 61 of error, optimize resources, and reduce patient risk. FDA recognizes the potential for these 62 technologies to provide significant benefits for enhancing the quality, availability, and safety of 63 medical devices, and has undertaken several efforts to help foster the adoption and use of such 64 technologies.   
65   
66 Specifically, FDA has engaged with stakeholders via the Medical Device Innovation Consortium 67 (MDIC), site visits to medical device manufacturers, and benchmarking efforts with other 68 industries (e.g., automotive, consumer electronics) to keep abreast of the latest technologies and 69 to better understand stakeholders’ challenges and opportunities for further advancement. As part 70 of these ongoing efforts, medical device manufacturers have expressed a desire for greater clarity 71 regarding the Agency’s expectations for software validation for computers and automated data 72 processing systems used as part of production or the quality system. Given the rapidly changing   
3 Available at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm.   
4 This guidance discusses the “intended use” of computer software used as part of production or the quality system (see 21 CFR 820.70(i)), which is different from the intended use of the device itself (see 21 CFR 801.4).  
5   
Contains Nonbinding Recommendations Draft – Not for Implementation   
73 nature of software, manufacturers have also expressed a desire for a more iterative, agile 74 approach for validation of computer software used as part of production or the quality system. 75   
76 Traditionally, software validation has often been accomplished via software testing and other 77 verification activities conducted at each stage of the software development lifecycle. However, 78 as explained in FDA’s Software Validation guidance, software testing alone is often insufficient 79 to establish confidence that the software is fit for its intended use. Instead, the Software 80 Validation guidance recommends that “software quality assurance” focus on preventing the 81 introduction of defects into the software development process, and it encourages use of a risk 82 based approach for establishing confidence that software is fit for its intended use. 83   
84 FDA believes that applying a risk-based approach to computer software used as part of 85 production or the quality system would better focus manufacturers’ assurance activities to help 86 ensure product quality while helping to fulfill the validation requirements of 21 CFR 820.70(i). 87 For these reasons, FDA is now providing recommendations on computer software assurance for 88 computers and automated data processing systems used as part of medical device production or 89 the quality system. FDA believes that these recommendations will help foster the adoption and 90 use of innovative technologies that promote patient access to high-quality medical devices and 91 help manufacturers to keep pace with the dynamic, rapidly changing technology landscape, while 92 promoting compliance with laws and regulations implemented by FDA.   
93   
94 III. Scope   
95 When final, this guidance is intended to provide recommendations regarding computer software 96 assurance for computers or automated data processing systems used as part of production or the 97 quality system.   
98   
99 This guidance is not intended to provide a complete description of all software validation 100 principles. FDA has previously outlined principles for software validation, including managing 101 changes as part of the software lifecycle, in FDA’s Software Validation guidance. This guidance 102 applies the risk-based approach to software validation discussed in the Software Validation 103 guidance to production or quality system software. This guidance additionally discusses specific 104 risk considerations, acceptable testing methods, and efficient generation of objective evidence 105 for production or quality system software.   
106   
107 This guidance does not provide recommendations for the design verification or validation 108 requirements specified in 21 CFR 820.30 when applied to software in a medical device (SiMD) 109 or software as a medical device (SaMD). For more information regarding FDA’s 110 recommendations for design verification or validation of SiMD or SaMD, see the Software 111 Validation guidance.   
112   
113 IV. Computer Software Assurance    
114 Computer software assurance is a risk-based approach for establishing and maintaining 115 confidence that software is fit for its intended use. This approach considers the risk of   
6   
Contains Nonbinding Recommendations Draft – Not for Implementation   
116 compromised safety and/or quality of the device (should the software fail to perform as intended) 117 to determine the level of assurance effort and activities appropriate to establish confidence in the 118 software. Because the computer software assurance effort is risk-based, it follows a least 119 burdensome approach, where the burden of validation is no more than necessary to address the 120 risk. Such an approach supports the efficient use of resources, in turn promoting product quality. 121   
122 In addition, computer software assurance establishes and maintains that the software used in 123 production or the quality system is in a state of control throughout its lifecycle (“validated 124 state”). This is important because manufacturers increasingly rely on computers and automated 125 processing systems to monitor and operate production, alert responsible personnel, and transfer 126 and analyze production data, among other uses. By allowing manufacturers to leverage 127 principles such as risk-based testing, unscripted testing, continuous performance monitoring, and 128 data monitoring, as well as validation activities performed by other entities (e.g., developers, 129 suppliers), the computer software assurance approach provides flexibility and agility in helping 130 to assure that the software maintains a validated state consistent with 21 CFR 820.70(i). 131   
132 Software that is fit for its intended use and that maintains a validated state should perform as 133 intended, helping to ensure that finished devices will be safe and effective and in compliance 134 with regulatory requirements (see 21 CFR 820.1(a)(1)). Section V below outlines a risk-based 135 framework for computer software assurance.   
136   
137 V. Computer Software Assurance Risk Framework    
138 The following approach is intended to help manufacturers establish a risk-based framework for 139 computer software assurance throughout the software’s lifecycle. Examples of applying this risk 140 framework to various computer software assurance situations are provided in Appendix A.   
141 Identifying the Intended Use    
142 The regulation requires manufacturers to validate software that is used as part of production or 143 the quality system for its intended use (see 21 CFR 820.70(i)). To determine whether the 144 requirement for validation applies, manufacturers must first determine whether the software is 145 intended for use as part of production or the quality system.   
146   
147 In general, software used as part of production or the quality system falls into one of two 148 categories: software that is used directly as part of production or the quality system, and software 149 that supports production or the quality system.   
150   
151 Software with the following intended uses are considered to be used directly as part of 152 production or the quality system:   
153   
154 ∙ Software intended for automating production processes, inspection, testing, or the 155 collection and processing of production data; and   
156 ∙ Software intended for automating quality system processes, collection and processing of 157 quality system data, or maintaining a quality record established under the Quality System 158 regulation.  
7   
Contains Nonbinding Recommendations Draft – Not for Implementation   
159   
160 Software with the following intended uses are considered to be used to support production or 161 the quality system:   
162   
163 ∙ Software intended for use as development tools that test or monitor software systems or 164 that automate testing activities for the software used as part of production or the quality 165 system, such as those used for developing and running scripts; and 166 ∙ Software intended for automating general record-keeping that is not part of the quality 167 record.   
168   
169 Both kinds of software are used as “part of” production or the quality system and must be 170 validated under 21 CFR 820.70(i). However, as further discussed below, supporting software 171 often carries lower risk, such that under a risk-based computer software assurance approach, the 172 effort of validation may be reduced accordingly without compromising safety. 173   
174 On the other hand, software with the following intended uses generally are not considered to be 175 used as part of production or the quality system, such that the requirement for validation in 21 176 CFR 820.70(i) would not apply:   
177   
178 ∙ Software intended for management of general business processes or operations, such as 179 email or accounting applications; and   
180 ∙ Software intended for establishing or supporting infrastructure not specific to production 181 or the quality system, such as networking or continuity of operations. 182   
183 FDA recognizes that software used in production or the quality system is often complex and comprised of several features, functions, and operations;5   
184 software may have one or more 185 intended uses depending on the individual features, functions, and operations of that software. In 186 cases where the individual features, functions, and operations have different roles within 187 production or the quality system, they may present different risks with different levels of 188 validation effort. FDA recommends that manufacturers examine the intended uses of the 189 individual features, functions, and operations to facilitate development of a risk-based assurance 190 strategy. Manufacturers may decide to conduct different assurance activities for individual 191 features, functions, or operations.   
192   
193 For example, a commercial off-the-shelf (COTS) spreadsheet software may be comprised of 194 various functions with different intended uses. When utilizing the basic input functions of the 195 COTS spreadsheet software for an intended use of documenting the time and temperature 196 readings for a curing process, a manufacturer may not need to perform additional assurance 197 activities beyond those conducted by the COTS software developer and initial installation and 198 configuration. The intended use of the software, “documenting readings,” only supports 199 maintaining the quality system record and poses a low process risk. As such, initial activities   
5 That is, software is often an integration of “features,” that are used together to perform a “function” that provides a desired outcome. Several functions of the software may, in turn, be applied together in an “operation” to perform practical work in a process. For the purposes of this guidance, a “function” refers to a “software function” and is not to be confused with a “device function.”  
8   
Contains Nonbinding Recommendations Draft – Not for Implementation   
200 such as the vendor assessment and software installation and configuration may be sufficient to 201 establish that the software is fit for its intended use and maintains a validated state. However, if a 202 manufacturer utilizes built-in functions of the COTS spreadsheet to create custom formulas that 203 are directly used in production or the quality system, then additional risks may be present. For 204 example, if a custom formula automatically calculates time and temperature statistics to monitor 205 the performance and suitability of the curing process, then additional validation by the 206 manufacturer might be necessary.   
207   
208 For the purposes of this guidance, we describe and recommend a computer software assurance 209 framework by examining the intended uses of the individual features, functions, or operations of 210 the software. However, in simple cases where software only has one intended use (e.g., if all of 211 the features, functions, and operations within the software share the same intended use), 212 manufacturers may not find it helpful to examine each feature, function, and operation 213 individually. In such cases, manufacturers may develop a risk-based approach and consider 214 assurance activities based on the intended use of the software overall.   
215   
216 FDA recommends that manufacturers document their decision-making process for determining 217 whether a software feature, function, or operation is intended for use as part of production or the 218 quality system in their Standard Operating Procedures (SOPs).   
219   
220 Determining the Risk­Based Approach   
221 Once a manufacturer has determined that a software feature, function, or operation is intended 222 for use as part of production or the quality system, FDA recommends using a risk-based analysis 223 to determine appropriate assurance activities. Broadly, this risk-based approach entails 224 systematically identifying reasonably foreseeable software failures, determining whether such a 225 failure poses a high process risk, and systematically selecting and performing assurance activities 226 commensurate with the medical device or process risk, as applicable.   
227   
228 Note that conducting a risk-based analysis for computer software assurance for production or 229 quality system software is distinct from performing a risk analysis for a medical device as 230 described in ISO 14971:2019 – Medical devices – Application of risk management to medical 231 devices. Unlike the risks contemplated in ISO 14971:2019 for analysis (medical device risks), 232 failures of the production or the quality system software to perform as intended do not occur in a 233 probabilistic manner where an assessment for the likelihood of occurrence for a particular risk 234 could be estimated based on historical data or modeling.   
235   
236 Instead, the risk-based analysis for production or quality system software considers those factors 237 that may impact or prevent the software from performing as intended, such as proper system 238 configuration and management, security of the system, data storage, data transfer, or operation 239 error. Thus, a risk-based analysis for production or quality system software should consider 240 which failures are reasonably foreseeable (as opposed to likely) and the risks resulting from each 241 such failure. This guidance discusses both process risks and medical device risks. A process risk 242 refers to the potential to compromise production or the quality system. A medical device risk 243 refers to the potential for a device to harm the patient or user. When discussing medical device   
9   
Contains Nonbinding Recommendations Draft – Not for Implementation   
244 risks, this guidance focuses on the medical device risk resulting from a quality problem that 245 compromises safety.   
246   
247 Specifically, FDA considers a software feature, function, or operation to pose a high process risk 248 when its failure to perform as intended may result in a quality problem that foreseeably 249 compromises safety, meaning an increased medical device risk. This process risk 250 identification step focuses only on the process, as opposed to the medical device risk posed to the 251 patient or user. Examples of software features, functions, or operations that are generally high 252 process risk are those that:   
253   
254 ∙ maintain process parameters (e.g., temperature, pressure, or humidity) that affect the 255 physical properties of product or manufacturing processes that are identified as essential 256 to device safety or quality;   
257   
258 ∙ measure, inspect, analyze and/or determine acceptability of product or process with 259 limited or no additional human awareness or review;   
260   
261 ∙ perform process corrections or adjustments of process parameters based on data 262 monitoring or automated feedback from other process steps without additional human 263 awareness or review;   
264   
265 ∙ produce directions for use or other labeling provided to patients and users that are 266 necessary for safe operation of the medical device; and/or   
267   
268 ∙ automate surveillance, trending, or tracking of data that the manufacturer identifies as 269 essential to device safety and quality.   
270   
271 In contrast, FDA considers a software feature, function, or operation not to pose a high process 272 risk when its failure to perform as intended would not result in a quality problem that 273 foreseeably compromises safety. This includes situations where failure to perform as 274 intended would not result in a quality problem, as well as situations where failure to 275 perform as intended may result in a quality problem that does not foreseeably lead to 276 compromised safety. Examples of software features, functions, or operations that generally are 277 not high process risk include those that:   
278   
279 ∙ collect and record data from the process for monitoring and review purposes that do not 280 have a direct impact on production or process performance;   
281   
282 ∙ are used as part the quality system for Corrective and Preventive Actions (CAPA) 283 routing, automated logging/tracking of complaints, automated change control 284 management, or automated procedure management;   
285   
286 ∙ are intended to manage data (process, store, and/or organize data), automate an existing 287 calculation, increase process monitoring, or provide alerts when an exception occurs in an 288 established process; and/or  
10   
Contains Nonbinding Recommendations Draft – Not for Implementation   
289   
290 ∙ are used to support production or the quality system, as explained in Section V.A. above. 291   
292 FDA acknowledges that process risks associated with software used as part of production or the 293 quality system are on a spectrum, ranging from high risk to low risk. Manufacturers should 294 determine the risk of each software feature, function, or operation as the risk falls on that 295 spectrum, depending on the intended use of the software. However, FDA is primarily concerned 296 with the review and assurance for those software features, functions, and operations that are high 297 process risk because a failure also poses a medical device risk. Therefore, for the purposes of this 298 guidance, FDA is presenting the process risks in a binary manner, “high process risk” and “not 299 high process risk.” A manufacturer may still determine that a process risk is, for example, 300 “moderate,” “intermediate,” or even “low” for purposes of determining assurance activities; in 301 such a case, the portions of this guidance concerning “not high process risk” would apply. As 302 discussed in Section V.C. below, assurance activities should be conducted for software that is 303 “high process risk” and “not high process risk” commensurate with the risk. 304   
305 Example 1: An Enterprise Resource Planning (ERP) Management system contains a feature that 306 automates manufacturing material restocking. This feature ensures that the right materials are 307 ordered and delivered to appropriate production operations. However, a qualified person checks 308 the materials before their use in production. The failure of this feature to perform as intended 309 may result in a mix-up in restocking and delivery, which would be a quality problem because the 310 wrong materials would be restocked and delivered. However, the delivery of the wrong materials 311 to the qualified person should result in the rejection of those materials before use in production; 312 as such, the quality problem should not foreseeably lead to compromised safety. The 313 manufacturer identifies this as an intermediate (not high) process risk and determines assurance 314 activities commensurate with the process risk. The manufacturer already undertakes some of 315 those identified assurance activities so implements only the remaining identified assurance 316 activities.   
317   
318 Example 2: A similar feature in another ERP management system performs the same tasks as in 319 the previous example except that it also automates checking the materials before their use in 320 production. A qualified person does not check the material first. The manufacturer identifies this 321 as a high process risk because the failure of the feature to perform as intended may result in a 322 quality problem that foreseeably compromises safety. As such, the manufacturer will determine 323 assurance activities that are commensurate with the related medical device risk. The 324 manufacturer already undertakes some of those identified assurance activities so implements 325 only the remaining identified assurance activities.   
326   
327 Example 3: An ERP management system contains a feature to automate product delivery. The 328 medical device risk depends upon, among other factors, the correct product being delivered to 329 the device user. A failure of this feature to perform as intended may result in a delivery mix-up, 330 which would be a quality problem that foreseeably compromises safety; as such, the 331 manufacturer identifies this as a high process risk. Since the failure would compromise safety, 332 the manufacturer will next determine the related increase in device risk and identify the 333 assurance activities that are commensurate with the device risk. In this case, the manufacturer   
11   
Contains Nonbinding Recommendations Draft – Not for Implementation   
334 has not already implemented any of the identified assurance activities so implements all of the 335 assurance activities identified in the analysis.   
336   
337 Example 4: An automated graphical user interface (GUI) function in the production software is 338 used for developing test scripts based on user interactions and to automate future testing of 339 modifications to the user interface of a system used in production. A failure of this GUI function 340 to perform as intended may result in implementation disruptions and delay updates to the 341 production system, but in this case, these errors should not foreseeably lead to compromised 342 safety because the GUI function operates in a separate test environment. The manufacturer 343 identifies this as a low (not high) process risk and determines assurance activities that are 344 commensurate with the process risk. The manufacturer already undertakes some of those 345 identified assurance activities so implements only the remaining identified assurance activities. 346   
347 As noted in FDA’s guidance, “30-Day Notices, 135 Day Premarket Approval (PMA) 348 Supplements and 75-Day Humanitarian Device Exemption (HDE) Supplements for Manufacturing Method or Process Changes,”6   
349 for devices subject to a PMA or HDE, changes to 350 the manufacturing procedure or method of manufacturing that do not affect the safety or 351 effectiveness of the device must be submitted in a periodic report (usually referred to as an annual report).7   
352 In contrast, modifications to manufacturing procedures or methods of 353 manufacture that affect the safety and effectiveness of the device must be submitted in a 30-day notice.8   
354 Changes to the manufacturing procedure or method of manufacturing may include 355 changes to software used in production or the quality system. For an addition or change to 356 software used in production or the quality system of devices subject to a PMA or HDE, FDA 357 recommends that manufacturers apply the principles outlined above in determining whether the 358 change may affect the safety or effectiveness of the device. In general, if a change may result in a 359 quality problem that foreseeably compromises safety, then it should be submitted in a 30-day 360 notice. If a change would not result in a quality problem that foreseeably compromises safety, an 361 annual report may be appropriate.   
362   
363 For example, a Manufacturing Execution System (MES) may be used to manage workflow, track 364 progress, record data, and establish alerts or thresholds based on validated parameters, which are 365 part of maintaining the quality system. Failure of such an MES to perform as intended may 366 disrupt operations but not affect the process parameters established to produce a safe and 367 effective device. Changes affecting these MES operations are generally considered annually 368 reportable. In contrast, an MES used to automatically control and adjust established critical 369 production parameters (e.g., temperature, pressure, process time) may be a change to a 370 manufacturing procedure that affects the safety or effectiveness of the device. If so, changes 371 affecting this specific operation would require a 30-day notice.   
372   
6 Available at https://www.fda.gov/regulatory-information/search-fda-guidance-documents/30-day-notices-135-day premarket-approval-pma-supplements-and-75-day-humanitarian-device-exemption.   
7 21 CFR 814.39(b), 814.126(b)(1), and https://www.fda.gov/regulatory-information/search-fda-guidance documents/annual-reports-approved-premarket-approval-applications-pma.   
8 21 CFR 814.39(b), 814.126(b)(1). Changes in manufacturing/sterilization site or to design or performance specifications do not qualify for a 30-day notice.   
12   
Contains Nonbinding Recommendations Draft – Not for Implementation   
373 Determining the Appropriate Assurance Activities    
374 Once the manufacturer has determined whether a software feature, function, or operation poses a 375 high process risk (a quality problem that may foreseeably compromise safety), the manufacturer 376 should identify the assurance activities commensurate with the medical device risk or the process 377 risk. In cases where the quality problem may foreseeably compromise safety (high process risk),   
378 the level of assurance should be commensurate with the medical device risk. In cases where the 379 quality problem may not foreseeably compromise safety (not high process risk), the level of 380 assurance rigor should be commensurate with the process risk. In either case, heightened risks of 381 software features, functions, or operations generally entail greater rigor, i.e., a greater amount of 382 objective evidence. Conversely, relatively less risk (i.e., not high process risk) of compromised 383 safety and/or quality generally entails less collection of objective evidence for the computer 384 software assurance effort.   
385   
386 A feature, function, or operation that could lead to severe harm to a patient or user would 387 generally be high device risk. In contrast, a feature, function, or operation that would not 388 foreseeably lead to severe harm would likely not be high device risk. In either case, the risk of 389 the software’s failure to perform as intended is commensurate with the resulting medical device 390 risk.   
391   
392 If the manufacturer instead determined that the software feature, function, or operation does not 393 pose a high process risk (i.e., it would not lead to a quality problem that foreseeably 394 compromises safety), the manufacturer should consider the risk relative to the process, i.e., 395 production or the quality system. This is because the failure would not compromise safety, so the 396 failure would not introduce additional medical device risk. For example, a function that collects 397 and records process data for review would pose a lower process risk than a function that 398 determines acceptability of product prior to human review.   
399   
400 Types of assurance activities commonly performed by manufacturers include, but are not limited 401 to, the following:   
402   
403 ∙ Unscripted testing – Dynamic testing in which the tester’s actions are not prescribed by written instructions in a test case.9   
404 It includes:   
405   
406 ∙ Ad-hoc testing – A concept derived from unscripted practice that focuses primarily 407 on performing testing that does not rely on large amounts of documentation (e.g., test procedures) to execute.10 408   
409   
410 ∙ Error-guessing – A test design technique in which test cases are derived on the basis of the tester’s knowledge of past failures or general knowledge of failure modes.11 411 412   
9IEC/IEEE/ISO 29119-1 First edition 2013-09-01: Software and systems engineering – Software testing - Part 1: Concepts and definitions, Section 4.94.   
10 Ibid., Section 5.6.5.   
11 Ibid., Section 4.14.  
13   
Contains Nonbinding Recommendations Draft – Not for Implementation   
413 ∙ Exploratory testing – Experience-based testing in which the tester spontaneously 414 designs and executes tests based on the tester’s existing relevant knowledge, prior 415 exploration of the test item (including results from previous tests), and heuristic 416 “rules of thumb” regarding common software behaviors and types of failure. 417 Exploratory testing looks for hidden properties, including hidden, unanticipated user 418 behaviors, or accidental use situations that could interfere with other software properties being tested and could pose a risk of software failure.12 419 420   
421 ∙ Scripted testing – Dynamic testing in which the tester’s actions are prescribed by written 422 instructions in a test case. Scripted testing includes both robust and limited scripted testing.13 423   
424   
425 ∙ Robust scripted testing – Scripted testing efforts in which the risk of the computer 426 system or automation includes evidence of repeatability, traceability to requirements, 427 and auditability.   
428   
429 ∙ Limited scripted testing – A hybrid approach of scripted and unscripted testing that 430 is appropriately scaled according to the risk of the computer system or automation. 431 This approach may apply scripted testing for high-risk features or operations and 432 unscripted testing for low- to medium-risk items as part of the same assurance effort. 433   
434 In general, FDA recommends that manufacturers apply principles of risk-based testing in which 435 the management, selection, prioritization, and use of testing activities and resources are 436 consciously based on corresponding types and levels of analyzed risk to determine the appropriate activities.14 437 For high-risk software features, functions, and operations, manufacturers 438 may choose to consider more rigor such as the use of scripted testing or limited scripted testing, 439 as appropriate, when determining their assurance activities. In contrast, for software features, 440 functions, and operations that are not high-risk, manufacturers may consider using unscripted 441 testing methods such as ad-hoc testing, error-guessing, exploratory testing, or a combination of 442 methods that is suitable for the risk of the intended use.   
443   
444 When deciding on the appropriate assurance activities, manufacturers should consider whether 445 there are any additional controls or mechanisms in place throughout the quality system that may 446 decrease the impact of compromised safety and/or quality if failure of the software feature, 447 function or operation were to occur. For example, as part of a comprehensive assurance 448 approach, manufacturers can leverage the following to reduce the effort of additional assurance 449 activities:   
450   
451 ∙ Activities, people, and established processes that provide control in production. Such 452 activities may include procedures to ensure integrity in the data supporting production or 453 software quality assurance processes performed by other organizational units. 454   
12 Ibid., Section 4.16.   
13 Ibid., Section 4.37.   
14 Ibid., Section 4.35.  
14   
Contains Nonbinding Recommendations Draft – Not for Implementation   
455 ∙ Established purchasing control processes for selecting and monitoring software 456 developers. For example, the manufacturer could incorporate the practices, validation 457 work, and electronic information already performed by developers of the software as the 458 starting point and determine what additional activities may be needed. For some lower 459 risk software features, functions, and operations, this may be all the assurance that is 460 needed by the manufacturer.   
461   
462 ∙ Additional process controls that have been incorporated throughout production. For 463 example, if a process is fully understood, all critical process parameters are monitored, 464 and/or all outputs of a process undergo verification testing, these controls can serve as 465 additional mechanisms to detect and correct the occurrence of quality problems that may 466 occur if a software feature, function, or operation were to fail to perform as intended. In 467 this example, the presence of these controls can be leveraged to reduce the effort of 468 assurance activities appropriate for the software.   
469   
470 ∙ The data and information periodically or continuously collected by the software for the 471 purposes of monitoring or detecting issues and anomalies in the software after 472 implementation of the software. The capability to monitor and detect performance issues 473 or deviations and system errors may reduce the risk associated with a failure of the 474 software to perform as intended and may be considered when deciding on assurance 475 activities.   
476   
477 ∙ The use of Computer System Validation tools (e.g., bug tracker, automated testing) for 478 the assurance of software used in production or as part of the quality system whenever 479 possible.   
480   
481 ∙ The use of testing done in iterative cycles and continuously throughout the lifecycle of 482 the software used in production or as part of the quality system.   
483   
484 For example, supporting software, as referenced in Section V.A., often carries lower risk, such 485 that the assurance effort may generally be reduced accordingly. Because assurance activities 486 used “directly” in production or the quality system often inherently cover the performance of 487 supporting software, assurance that this supporting software performs as intended may be 488 sufficiently established by leveraging vendor validation records, software installation, or 489 software configuration, such that additional assurance activities (e.g., scripted or unscripted 490 testing) may be unnecessary.   
491   
492 Manufacturers are responsible for determining the appropriate assurance activities for ensuring 493 the software features, functions, or operations maintain a validated state. The assurance activities 494 and considerations noted above are some possible ways of providing assurance and are not 495 intended to be prescriptive or exhaustive. Manufacturers may leverage any of the activities or a 496 combination of activities that are most appropriate for risk associated with the intended use. 497  
15   
Contains Nonbinding Recommendations Draft – Not for Implementation   
498 Establishing the Appropriate Record   
499 When establishing the record, the manufacturer should capture sufficient objective evidence to 500 demonstrate that the software feature, function, or operation was assessed and performs as 501 intended. In general, the record should include the following:   
502   
503 ∙ the intended use of the software feature, function, or operation;   
504 ∙ the determination of risk of the software feature, function, or operation; 505 ∙ documentation of the assurance activities conducted, including:   
506 ∙ description of the testing conducted based on the assurance activity; 507 ∙ issues found (e.g., deviations, failures) and the disposition; 508 ∙ conclusion statement declaring acceptability of the results; 509 ∙ the date of testing/assessment and the name of the person who conducted the 510 testing/assessment;   
511 ∙ established review and approval when appropriate (e.g., when necessary, a 512 signature and date of an individual with signatory authority) 513   
514 Documentation of assurance activities need not include more evidence than necessary to show 515 that the software feature, function, or operation performs as intended for the risk identified. FDA 516 recommends the record retain sufficient details of the assurance activity to serve as a baseline for improvements or as a reference point if issues occur.15 517   
518   
519 Table 1 provides some examples of ways to implement and develop the record when using the 520 risk-based testing approaches identified in Section V.C. above. Manufacturers may use 521 alternative approaches and provide different documentation so long as their approach satisfies 522 applicable legal documentation requirements.   
523   
524 Table 1 – Examples of Assurance Activities and Records   
  
  
15 For the Quality System regulation’s general requirements for records, including record retention period, see 21 CFR 820.180.  
16   
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
  
  
525 526 527 528  
17   
Contains Nonbinding Recommendations Draft – Not for Implementation   
529 The following is an example of a record of assurance in a scenario where a manufacturer has 530 developed a spreadsheet with the intended use of collecting and graphing nonconformance data 531 stored in a controlled system for monitoring purposes. In this example, the manufacturer has 532 established additional process controls and inspections that ensure non-conforming product is not 533 released. In this case, failure of the spreadsheet to perform as intended would not result in a 534 quality problem that foreseeably leads to compromised safety, so the spreadsheet would not pose 535 a high process risk. The manufacturer conducted rapid exploratory testing of specific functions 536 used in the spreadsheet to ensure that analyses can be created, read, updated, and/or deleted. 537 During exploratory testing, all calculated fields updated correctly except for one deviation that 538 occurred during update testing. In this scenario, the record would be documented as follows: 539   
540 ∙ Intended Use: The spreadsheet is intended for use in collecting and graphing 541 nonconformance data stored in a controlled system for monitoring purposes; as such, it is 542 used as part of production or the quality system. Because of this use, the spreadsheet is 543 different from similar software used for business operations such as for accounting. 544   
545 ∙ Risk-Based Analysis: In this case, the software is only used to collect and display data 546 for monitoring nonconformances, and the manufacturer has established additional process 547 controls and inspections to ensure that nonconforming product is not released. Therefore, 548 failure of the spreadsheet to perform as intended should not result in a quality problem 549 that foreseeably leads to compromised safety. As such, the software does not pose a high 550 process risk, and the assurance activities should be commensurate with the process risk. 551   
552 ∙ Tested: Spreadsheet X, Version 1.2   
553   
554 ∙ Test type: Unscripted testing – exploratory testing   
555   
556 ∙ Goal: Ensure that analyses can be correctly created, read, updated, and deleted 557   
558 ∙ Testing objectives and activities:   
559   
560 o Create new analysis – Passed   
561 o Read data from the required source – Passed   
562 o Update data in the analysis – Failed due to input error, then passed 563 o Delete data – Passed   
564 o Verify through observation that all calculated fields correctly update with changes 565 – Passed with noted deviation   
566   
567 ∙ Deviation: During update testing, when the user inadvertently input text into an 568 updatable field requiring numeric data, the associated row showed an immediate error. 569   
570 ∙ Conclusion: No errors were observed in the spreadsheet functions beyond the deviation. 571 Incorrectly inputting text into the field is immediately visible and does not impact the risk 572 of the intended use. In addition, a validation rule was placed on the field to permit only 573 numeric data inputs.  
18   
Contains Nonbinding Recommendations Draft – Not for Implementation   
574   
575 ∙ When/Who: July 9, 2019, by Jane Smith   
576   
577 Advances in digital technology may allow for manufacturers to leverage automated traceability, 578 testing, and the electronic capture of work performed to document the results, reducing the need 579 for manual or paper-based documentation. As a least burdensome method, FDA recommends the   
580 use of electronic records, such as system logs, audit trails, and other data generated by the 581 software, as opposed to paper documentation and screenshots, in establishing the record 582 associated with the assurance activities.   
583   
584 Manufacturers have expressed confusion and concern regarding the application of Part 11, 585 Electronic Records; Electronic Signatures, to computers or automated data processing systems 586 used as part of production or the quality system. As described in the “Part 11, Electronic Records; Electronic Signatures – Scope and Application” guidance,16 587 the Agency intends to 588 exercise enforcement discretion regarding Part 11 requirements for validation of computerized 589 systems used to create, modify, maintain, or transmit electronic records (see 21 CFR 11.10(a) 590 and 11.30). In general, Part 11 applies to records in electronic form that are created, modified, 591 maintained, archived, retrieved, or transmitted under any records requirements set forth in 592 Agency regulations (see 21 CFR 11.1(b)). Part 11 also applies to electronic records submitted to 593 the Agency under requirements of the Federal Food, Drug, and Cosmetic Act (FD&C Act) and 594 the Public Health Service Act (PHS Act), even if such records are not specifically identified in 595 Agency regulations (see 21 CFR 11.1(b)).   
596   
597 In the context of computer or automated data processing systems, for computer software used as 598 part of production or the quality system, a document required under Part 820 and maintained in 599 electronic form would generally be an “electronic record” within the meaning of Part 11 (see 21   
600 CFR 11.3(b)(6)). For example, if a document requires a signature under Part 820 and is 601 maintained in electronic form, then Part 11 applies (see, e.g., 21 CFR 820.40 (requiring 602 signatures for control of required documents)).   
16 https://www.fda.gov/regulatory-information/search-fda-guidance-documents/part-11-electronic-records electronic-signatures-scope-and-application.  
19   
603 Appendix A. Examples   
Contains Nonbinding Recommendations Draft – Not for Implementation   
604 The examples in this section outline possible application of the principles in this draft guidance to various software assurance 605 situations cases.   
606 Example 1: Nonconformance Management System   
607 A manufacturer has purchased COTS software for automating their nonconformance process and is applying a risk-based approach for 608 computer software assurance in its implementation. The software is intended to manage the nonconformance process electronically. 609 The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy: 610   
611 Table 2. Computer Software Assurance Example for a Nonconformance Management System  
  
  
20   
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
  
  
21  
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
  
  
612 613 614 615   
616  
22   
Contains Nonbinding Recommendations Draft – Not for Implementation   
617 Example 2: Learning Management System (LMS)   
618 A manufacturer is implementing a COTS LMS and is applying a risk-based approach for computer software assurance in its 619 implementation. The software is intended to manage, record, track, and report on training. The following features, functions, or 620 operations were considered by the manufacturer in developing a risk-based assurance strategy:   
621   
622 Table 3. Computer Software Assurance Example for an LMS   
  
  
623   
624  
23   
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
625 Example 3: Business Intelligence Applications   
626 A medical device manufacturer has decided to implement a commercial business intelligence solution for data mining, trending, and 627 reporting. The software is intended to better understand product and process performance over time, in order to provide identification 628 of improvement opportunities. The following features, functions, or operations were considered by the manufacturer in developing a 629 risk-based assurance strategy:   
630   
631 Table 4. Computer Software Assurance Example for a Business Intelligence Application  
  
  
24   
Contains Nonbinding Recommendations   
Draft – Not for Implementation   
  
  
632  
25   
  
--- Risk Levels.docx ---  
Risk Levels:  
BR 9.2 – Low Risk  
BR 4.3 – Low Risk  
BR 3.1 – Low Risk  
BR 4.50 – Low Risk  
BR 7.2 – Low Risk  
BR 10.1 – Low Risk  
BR 8.1 – High Risk  
UR-REG-36 – High Risk  
UR-REG-05 - High Risk  
UR-REG-13 - High Risk  
UR-REG-22 - High Risk  
UR-REG-03 - High Risk  
BR 1.3 – Low Risk  
BR 4.9 – Low Risk  
  
  
  
--- Test Plan Template.docx ---  
Test Plan  
  
  
<System Name>  
  
<CR ####>  
  
  
Document Approval  
The electronic signatures for this document are maintained in an electronic document management system, myCIMS. This should not be considered an approved document and used for reference unless the signature page from that system is attached.  
  
Revision History  
The revision history for this document is maintained in an electronic document management system, myCIMS.  
  
Purpose  
<Refer to PRCD-104040, Test Plan section for details>  
Definitions  
<Refer to PRCD-104040, Test Plan section for details>   
List in alphabetical order the terms, acronyms, and abbreviations used in the body of this document and which would not be understood by a reader unfamiliar with the system being documented  
Roles   
<Refer to PRCD-104040, Validation Plan section for details>  
The following roles have been identified for this project:  
  
  
  
  
  
  
  
  
  
  
  
The specific roles identified in the validation effort are not necessarily the final approvers of this plan.   
Testing Overview  
Testing Scope  
<Refer to PRCD-104040, Test Plan section for details.>  
Risks and Assumptions  
<Refer to PRCD-104040, Test Plan section for details. The risks and assumptions listed in this section are relevant to the execution of the testing applicable to this test plan. For each risk provide a mitigation. (e.g., Risk – Changes is requirement documents may result in additional effort to test design and execution. Mitigation – Assess the requirement specification for mitigation). >  
Out of Scope  
<Mark as N/A if this section is not needed>  
Test Strategy  
Test Outline  
<Refer to PRCD-104040, Test Plan section for details. Define the testing tool that will be utilized (electronic or manual). Define the required test types (e.g., IQ, OQ, UAT) and their order. More detail in the following sub-section>  
Vendor Testing  
<Mark as N/A if this section is not needed. Determine how vendor tests will be leveraged. Per Biogen procedures Vendor testing cannot be leveraged for high-risk requirements>  
Integration Testing  
< Mark as N/A if this section is not needed. Determine where regression testing will occur. (e.g., IQ, OQ) >  
Regression Testing  
< Mark as N/A if this section is not needed. Define if regression testing suites need to be ulilized or updated. Determine where regression testing will occur. (e.g., OQ) >  
Backup and Restore  
< Mark as N/A if this section is not needed>  
Environments  
<Refer to PRCD-104040, Test Plan section for details. As applicable, define where Dry Run testing should be performed (non-production).>  
Testing  
< In the Sub-sections below, per Test Type (e.g., IQ, OQ, UAT) define the objective, risks and assumption, dependencies, and acceptance criteria pertaining to each execution >  
Test Type - <Installation Qualification>  
<This Section should be renamed to the Test Protocol that is described. (e.g., Installation Qualification Pre-Production, Operational Qualification) For each Test Type, defined in the Testing Section, add a new sub-section.>  
Purpose and Scope  
<Define the purpose of the respective test type.(i.e, The IQ provides documented assurance that the system is installed per specifications.) Define the functionality tested as part of the this test type. (i.e., regression tests, new functions, hardware verification, software install verification ).>   
Dependencies  
<Mark as N/A if this section is not needed >  
Acceptance Critieria  
<Mark as N/A if this section is not needed >  
Test Type - <Operational Qualification>  
<This Section should be renamed to the Test Protocol that is described. (e.g., Installation Qualification Pre-Production, Operational Qualification) For each Test Type, defined in the Testing Section, add a new sub-section.>  
Purpose and Scope  
<Define the purpose of the respective test type.(i.e, The IQ provides documented assurance that the system is installed per specifications.) Define the functionality tested as part of the this test type. (i.e., regression tests, new functions, hardware verification, software install verification ).>   
Dependencies  
<Mark as N/A if this section is not needed >  
Acceptance Critieria  
<Mark as N/A if this section is not needed >  
Test Type - <User Acceptance Testing>  
<This Section should be renamed to the Test Protocol that is described. (e.g., Installation Qualification Pre-Production, Operational Qualification) For each Test Type, defined in the Testing Section, add a new sub-section.>  
Purpose and Scope  
<Define the purpose of the respective test type.(i.e, The IQ provides documented assurance that the system is installed per specifications.) Define the functionality tested as part of the this test type. (i.e., regression tests, new functions, hardware verification, software install verification ).>   
Dependencies  
<Mark as N/A if this section is not needed >  
Acceptance Critieria  
<Mark as N/A if this section is not needed >  
Test Data  
<Refer to PRCD-104040, Test Plan section for details>   
Defect Management  
< Reference PRCD-19193, IT Test Incident Reporting (TIR)>  
References  
References should include your System Assessment (SA), Validation Plan, Risk Assessment if one is required, and other documents as needed to understand the document. In particular, any artifact that scopes or informs the test strategy should be listed here.  
  
Appendix A: IQ Test Scripts   
Provide a listing of test scripts to be executed. This list is often done in an updated version of the Test Plan when the exact scope of testing is more precisely defined  
Installation Qualification (IQ)  
 Domain : POIT  
Project : <System Name>  
IQ Path : Test Plan > Subject > <IQ>  
  
Appendix B: OQ Test Scripts  
Provide a listing of test scripts to be executed. This list is often done in an updated version of the Test Plan when the exact scope of testing is more precisely defined  
Operational Qualification (OQ) -<Phase 1>  
Domain: POIT   
Project : <System Name>   
Path : Test Plan > Subject > <OQ>   
  
Operational Qualification (OQ) - <Phase 2>  
Provide a listing of test scripts to be executed. This list is often done in an updated version of the Test Plan when the exact scope of testing is more precisely defined  
Domain: POIT   
Project : <System Name>   
Path : Test Plan > Subject > <OQ>   
  
Appendix C: UAT Test Scripts  
Provide a listing of test scripts to be executed. This list is often done in an updated version of the Test Plan when the exact scope of testing is more precisely defined  
  
User Acceptance Testing (UAT)  
Domain: IO\_IT  
Project: <System Name>  
MW IQ Path: Test Plan > Subject > < UAT>  
  
  
  
  
  
--- Trace Matrix v8.docx ---  
Start of general requirements:  
  
BR 1.4  
The system shall allow for routing functionality within the application.  
FR 6.1.1  
The system will contain new workflow, menu and security group configuration.  
BR 4.10  
The system will have ability to assign multiple pieces of equipment to a work order.   
FR 6.1.2  
The system will ensure that the equipment location on PM schedules will stay current with the location on the equipment record.  
BR 1.8  
The system shall have the capability to configure field name labels, where appropriate, in order to comply with corporate nomenclature.  
FR 6.1.4  
All displayed dates should be of the format “DD-MMM-YYYY”.  
BR 1.8  
The system shall have the capability to configure field name labels, where appropriate, in order to comply with corporate nomenclature  
FR 6.1.5  
Whenever time is displayed or entered the 24-hr clock should be used.  
BR 10.1  
The system shall provide the ability to interface with active directory.   
BR 10.1 Test Script: 143  
BR 3.8  
The system shall be able to route and track revisions to preventative maintenance plans.  
FR 6.1.10  
The system will have a revision approval process for PM Schedules, Job Plans, Material Lists, and Routes.   
BR 3.10  
The system shall be able to calculate due dates for preventive maintenance.  
FR 6.1.11  
The system will provide the ability to correctly calculate preventative maintenance due dates based on PM Schedule frequency, PM Schedule revisions, and PM Extensions.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.   
BR 8.1 Test Script: 65  
FR 6.2.2  
The system will provide the ability to separate data by organization (site), allowing some users access only to their local data, while allowing authorized users to view all data within the database. This viewing will be permitted through validated system screens and reports only.  
BR 1.12  
Ability for users to personalize home page with KPI’s and Inboxes  
FR 6.2.4  
Individual system users will be able to customize their home page with relevant inbox and key performance indicators (KPI) information.  
BR 1.13  
Ability to search for users by User Group.  
FR 6.1.12  
The system will allow users to search for other users in the system by using a lookup grid containing these fields: User Code, Employee ID, User Description, Role, Org, Default Org, and Out of Service.  
BR 1.14  
The system shall control and store the list of equipment validated for use in manufacturing a specific product (BOE)  
FR 6.1.13  
The system enables authorized users to generate Bill of Equipment records detailing lists of Equipment validated for use in manufacturing a specific product and the status of the Equipment; as well as to associate the Equipment on the BOE with the attribute settings required by the BOE.  
BR 1.15  
The system shall control and store product-specific manufacturing parameters (attribute settings).  
FR 6.1.14  
A settings tab on the BOE will detail existing Equipment attribute settings relevant to manufacture of the corresponding product.  
BR 1.16  
The system shall allow the user to select the equipment to be used for a manufacturing campaign from the BOE. (IEL)  
FR 6.1.15  
A button will be available on Equipment Change Request (ECR) records to populate the Incoming Equipment List (IEL) from the corresponding BOE.  
BR 1.17  
The system shall assert SME Review of all BOE and attribute changes.  
FR 6.1.16  
BOE will be revision controlled and support an SME review status prior to approval.  
BR 1.18  
The system shall assert QA Review of all BOE with settings listed in PCD.  
FR 6.1.17  
BOE will be revision controlled and applicable BOE will support a QA review status prior to approval, independent of the Type values assigned to Settings on the BOE.  
BR 1.6  
Users shall be able to define and save viewing properties (Dataspy).  
FR 6.2.5  
The system will allow users to alter the viewing structure of screens, such as equipment, job plans (task instructions), preventive maintenance (PM) routines and work orders. The system must also allow users to save the altered layout for future use.  
BR 1.6  
Users shall be able to define and save viewing properties (Dataspy).  
FR 6.2.6  
Individual system users will be able to define and save screen filters and data sorts.  
BR 1.7  
The system shall be able to store and attach electronic documents throughout the application.  
FR 6.2.7  
The system will allow for the storage and attachment of documents, images, and drawings to records such as equipment, work orders, PMs, parts, requisitions, and vendors.  
BR 1.8  
The system shall have the capability to configure field name labels, where appropriate, in order to comply with corporate nomenclature.  
FR 6.2.8  
The system will allow for the configuration of field name labels as appropriate to comply with corporate nomenclature.  
BR 3.1  
The system shall allow for the creation /modify of equipment, systems, and locations, as well as associated detailed information for each equipment record.   
BR 3.1  
The system shall allow for the creation /modify of equipment, systems, and locations, as well as associated detailed information for each equipment record.   
FR 6.3.2  
The system will be able to maintain equipment records with ID/Equipment numbers up to 20 characters long.  
BR 3.5  
The system shall be able to store equipment numbers and corresponding detailed information  
FR 6.3.4  
The system will allow read-only viewing of equipment move transactions into or out of a location.  
BR 3.5  
The system shall be able to store equipment numbers and corresponding detailed information  
FR 6.3.5  
The system will be able to identify equipment as GMP or non-GMP, direct or indirect, and critical or non-critical.  
BR 3.3  
The system shall have the ability to create and maintain a parent – child hierarchy.  
FR 6.3.6  
The system will allow the creation and/or viewing of equipment hierarchies.  
BR 3.4  
The system shall have the ability to create and maintain a spare parts list for each equipment item.  
FR 6.3.7  
The system will be able to create and maintain a spare parts list for each equipment item.  
BR 3.2  
The system shall have the ability to differentiate between Equipment classifications  
FR 6.3.8  
The system will be able to store equipment numbers and corresponding information such as description, type, make, model, serial number, classification, location, system number, vendor, old equipment number, operating status, process and instrumentation diagram (P&ID) tag numbers, P&ID drawing numbers, assigned cost center, and a history of maintenance costs.  
BR 3.6  
The system shall be able to store closing codes to construct accurate histories of the failures that affect equipment and operating locations  
FR 6.3.9  
The system will be able to store failure code to assist in the diagnosis of failures that affect equipment and operating locations.  
BR 3.6  
The system shall be able to store closing codes to construct accurate histories of the failures that affect equipment and operating locations  
FR 6.3.10  
The system will allow the association of failure codes to work orders so that failure trends can be captured and analyzed.  
BR 3.7  
The system shall provide the capability to maintain preventive maintenance records, and associate them with equipment and locations  
FR 6.4.1  
System PM Schedule records will allow for the addition, modification, and deletion of such information as, description, classification, schedule/due dates, equipment and trade requirements.  
BR 3.9  
The user shall be able to associate a job plan (task instruction) with each PM record.  
FR 6.4.2  
The system will have the ability to create, revise, and view job plan instructions.  
BR 3.7  
The system shall provide the capability to maintain preventive maintenance records, and associate them with equipment and locations  
FR 6.4.3  
The system will allow a PM frequency to be specified in days, weeks, months, or years.  
BR 3.8  
The system shall be able to route and track revisions to preventative maintenance plans.  
FR 6.4.4  
The system will be able to track revisions for PM entities..   
BR 3.7  
The system shall provide the capability to maintain preventive maintenance records, and associate them with equipment and locations  
FR 6.4.5  
The system will be able to associate PM schedules with job plan instructions, material lists, attached documents, estimated labor, and tools.  
BR 3.9  
The user shall be able to associate a job plan (task instruction) with each PM record.  
FR 6.4.6  
The system will allow the viewing, addition, modification, and deactivation of job plan records.  
BR 4.3  
The system shall allow the authorized user to plan, create, reject, review, modify, approve, and cancel work orders against equipment, as well as locations.   
FR 6.4.7  
The system will have the ability to calculate scheduled due dates from defined preventive maintenance intervals based on prior scheduled due date or prior work order completion date.  
BR 4.1  
The system shall allow the Company A corporate intranet authorized user community to create work requests in the system.  
FR 6.4.8  
The system will allow authorized users to create work requests via the Company A intranet.  
BR 4.2  
The system shall allow the Company A corporate intranet authorized user community to check the status of any work request.  
FR 6.4.9  
The system will allow authorized Company A corporate intranet users to check the status of the work requests that they have submitted.  
BR 4.3  
The system shall allow the authorized user to plan, create, reject, review, modify, approve, and cancel work orders against equipment, as well as locations.   
FR 6.4.10  
The system will allow authorized users to plan, create, review, reject, modify, approve, and cancel work orders and work requests for equipment and/or locations.  
BR 4.8  
The system shall be configurable to incorporate multiple work flows for various types of work and their associated processes  
FR 6.4.11  
The system will allow processing of work orders to route, complete, review, approve, and close, in compliance with the business processes.  
BR 3.1  
The system shall allow for the creation /modify of equipment, systems, and locations, as well as associated detailed information for each equipment record.   
FR 6.4.12  
BR 3.9  
The user shall be able to associate a job plan (task instruction) with each PM record.  
FR 6.4.13  
The system will be able to maintain job plan descriptions.   
BR 4.41  
The system shall provide a means to generate work orders based on meter reading.  
FR 6.4.14  
The system will be able to release PM work orders from meter readings or inspection results.   
BR 4.11  
The system shall allow authorized users to generate work orders and requisitions.  
FR 6.4.15  
The system will have the ability to generate work orders to track preventive and corrective maintenance for systems, equipment, and/or locations.  
BR 4.4  
The system shall allow authorized users to generate work orders from a preventive maintenance schedule.  
FR 6.4.16  
The system will be able to generate preventive maintenance work orders from the PM schedule.  
BR 3.3  
The system shall have the ability to create and maintain a parent – child hierarchy.  
FR 6.4.17  
The system will be able to create and maintain parent-child work order hierarchies.   
BR 4.6  
The system shall be able to associate various work order types and priorities to specific tasks or work requests.  
FR 6.4.19  
The system will allow for the specification of the following work order types:  
BR - Breakdown Maintenance  
PM - Preventive Maintenance  
CM - Corrective Maintenance  
RM - Routine Maintenance  
BR - Breakdown Maintenance  
PM - Preventive Maintenance  
CM - Corrective Maintenance.  
RM - Routine Maintenance  
BR 3.1  
The system shall allow for the creation /modify of equipment, systems, and locations, as well as associated detailed information for each equipment record.   
FR 6.4.20  
The system will be able to identify if a piece of equipment or location on a PM or work order is GMP if QA Oversight is triggered by FLEX and checked.  
BR 4.8  
The system shall be configurable to incorporate multiple work flows for various types of work and their associated processes  
FR 6.4.21  
The system will be configurable to incorporate multiple work order flows for various types of work and their associated processes such as PM, work order requests, GMP, non-GMP, safety issues, and critical work orders.  
BR 4.9  
The system shall be capable of scheduling work by individual and/or trade.  
FR 6.4.22  
The system will be able to schedule work and assign labor trade requirements.  
BR 1.7  
The system shall be able to store and attach electronic documents throughout the application.  
FR 6.4.23  
The system will allow creation and viewing of attached documents.  
BR 1.4  
The system shall allow for routing functionality within the application.  
FR 6.4.25  
The system will give authorized users the ability to notify personnel associated with work on a piece of equipment for which there may be impending safety concerns.  
BR 1.4  
The system shall allow for routing functionality within the application.  
FR 6.4.26  
The system will notify members of the EHS (Environmental Health & Safety) group when work requests with safety implications are created.  
BR 5.9  
The system shall be able to reserve material requirements to scheduled or unscheduled work orders and provide visibility to the reservation.  
FR 6.5.2  
The system will allow authorized users to check the status of any CMMS generated parts request.   
BR 3.1  
The system shall allow for the creation /modify of equipment, systems, and locations, as well as associated detailed information for each equipment record.   
FR 6.5.4  
System item records will include the incorporation of such information as item/part number, description, manufacturer, manufacturer item number, vendor, vendor part number, general ledger, reorder point, lead time, unit of issue, unit of purchase, and cost. Functionality will be turned on at a future date if required  
BR 5.3  
The system shall be able to maintain inventory items that are stocked in one or more storerooms.  
FR 6.5.6  
The system will be capable of controlling inventory items by lot number and/or expiration date. Functionality will be turned on at a future date if required  
BR 5.16  
The system shall have the capability to track parts as Equipment/repairable spares  
FR 6.5.7  
The system will be able to monitor inventory items by serial number. Functionality will be turned on at a future date if required  
BR 5.3  
The system shall be able to maintain inventory items that are stocked in one or more storerooms.   
FR 6.5.8  
The system will allow items to be stored in multiple bins.   
BR 5.18  
Bin information will show current stock level and last physical count date. Functionality will be turned on at a future date if required.  
FR 6.5.9  
Bin information will show current stock level and last physical count date  
BR 5.19  
The system shall allow authorized users to override the automatic population of “Preferred Supplier” information on the “Stores” tab of Part records.  
FR 6.5.22  
Administrator User Groups will be allowed to override the automatic population of “Preferred Supplier” field on the “Stores” tab of Part records through manual editing of the field’s contents.  
BR 5.3  
The system shall be able to maintain inventory items that are stocked in one or more storerooms.   
FR 6.5.10  
The system will be able to maintain inventory information for multiple storerooms.  
BR 5.4  
The system shall be able to create and maintain main and satellite storerooms, and their associations.  
BR 5.5  
The system shall be able to track multiple vendor and manufacturer information for each inventory item.   
FR 6.5.12  
The system will be able to maintain multiple vendor and manufacturer listings for each inventory item record.  
BR 5.6  
The system shall be able to create and maintain rotating (repairable) equipment.  
FR 6.5.13  
The system will be able to create and maintain rotating (repairable) equipment.  
BR 5.7  
The system shall be able to issue/return inventory parts to Work Orders and Equipment  
FR 6.5.14  
The system will allow the issuance, receipt, and return of parts to/from a work order, equipment.   
BR 5.8  
The system shall be able to associate parts to equipment, to a building, or to a defined area.   
FR 6.5.15  
The system will be able to associate parts to equipment, system, or location.  
BR 5.9  
The system shall be able to reserve material requirements to scheduled or unscheduled work orders and provide visibility to the reservation.  
FR 6.5.16  
The system will be able to reserve materials requirements to scheduled or unscheduled work orders and provide visibility to the reservation.  
BR 5.10  
The system shall be able to provide inventory availability based on quantity in hand, quantity reserved, quantity awaiting repair, or quantity on order.  
FR 6.5.17  
The system will be able to provide inventory availability based on quantity on hand, quantity reserved, and quantity on order.   
BR 5.11  
The system shall provide authorized users the ability to run real-time part availability checks.  
FR 6.5.18  
The system will provide the ability to run real-time material availability checks.  
BR 5.12  
The system shall allow authorized users to view the transaction history of items.  
FR 6.5.19  
The system will allow the tracking of all inventory transactions, such as store-to-store and/or bin-to-bin transfers, and receipt of stocked, non-stocked, and special order items.  
BR 5.13  
The system shall have the capability to do inventory cycle count.  
FR 6.5.20  
The system will have the ability to perform a cycle count or physical inventory.   
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure  
FR 6.6.1  
The system will be able to indicate a purchase unit of measure, which can be different from the consumption unit of measure.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure  
FR 6.6.2  
The system will be able to indicate the conversion used between purchase unit of measure and consumption unit of measure.  
BR 6.1  
The system shall be capable of integrating with Oracle Purchasing application for the generation of vendor records, and purchase orders, as well as the receipt of materials, and viewing of purchase order balances.  
FR 6.6.3  
The system will allow the viewing of vendor records containing relevant information such as vendor code, description, and other specific data.  
BR 6.1  
The system shall be capable of integrating with Oracle Purchasing application for the generation of vendor records, and purchase orders, as well as the receipt of materials, and viewing of purchase order balances.  
FR 6.6.4  
The system will be able to prioritize vendors that are assigned to parts.  
BR 6.1  
The system shall be capable of integrating with Oracle Purchasing application for the generation of vendor records, and purchase orders, as well as the receipt of materials, and viewing of purchase order balances.  
FR 6.6.5  
The system will be able to associate multiple vendors to each part, with the ability to indicate a default vendor.  
BR 6.1  
The system shall be capable of integrating with Oracle Purchasing application for the generation of vendor records, and purchase orders, as well as the receipt of materials, and viewing of purchase order balances.  
FR 6.6.6  
The system will be able to associate multiple shipping address information to each vendor record.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.  
FR 6.7.1  
The system will have multi-level security to limit user access.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.  
FR 6.7.2  
The system will allow read-only access and be able to disallow access to tables and modules that are not part of the user functional job description.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.  
FR 6.7.3  
Configuration of security access levels will include the ability to define security filters associated with users, roles, and workflows.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.  
FR 6.7.4  
CMMS system administrators will be able to add/inactivate users, change user security settings, and add/inactivate reports within the system.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.  
FR 6.7.6  
The system will allow the definition and configuration of user groups to differentiate security access levels.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.  
FR 6.7.7  
The system will allow configuration of security access at the record/table level in regards to record inserts, updates, and deletes.  
BR 8.1  
The system shall provide security to allow or disallow functionality on the system level, site level, and user level.  
FR 6.7.9  
The system will allow configuration of a field to provide the last date and time a user has accessed the system.  
BR 1.5  
The system shall allow for user profiles  
FR 6.8.1  
The employee record in CMMS will include employee name, organization/location, and phone number.   
BR 9.2  
The system will create requestor user accounts by integrating into active directory  
FR 6.8.3  
The system will be capable of integrating with the authoritative source of employee and contractor data (i.e., Workday or Fieldglass) for access to corporate employee record information.  
BR 9.1  
The system shall be able to track employees by trades  
FR 6.8.4  
The system will be able to track labor by multiple occupation types/burden rates.  
BR 10.1  
The system shall provide the ability to interface with active directory  
FR 6.9.1  
The system will provide the ability to perform batch updates to CMMS employee data and cost center information from the authoritative source of employee and contractor data (i.e., Workday or Fieldglass).  
BR 10.1  
The system shall provide the ability to interface with active directory  
ITPD-38444  
GFR-004  
BR 10.1  
The system shall provide the ability to interface with active directory  
ITPD-38444 GFR-005  
The interface processes scheduled transmissions of Employee Data and delivers the packets to Infor  
BR 3.1  
The system shall allow for the creation /modify of equipment, systems, and locations, as well as associated detailed information for each equipment record.   
FR 6.9.4  
The requestor will be able to retrieve equipment and location information from the CMMS system.  
BR 9.2  
The system will create requestor user accounts by integrating into active directory  
FR 6.9.5  
All Company A personnel (employees, temps, contractors, interns, etc.) will be able to submit a work request from any Company A workstation in CMMS without having to request an application user account.  
BR 1.4  
The system shall allow for routing functionality within the application.  
FR 6.9.6  
The system shall be designed such that work requests can be input into one queue based on user login and then automatically routed to the appropriate site for review and approval.  
BR 4.2  
The system shall allow the Company A corporate intranet authorized user community to check the status of any work request.  
FR 6.9.7  
The system shall be designed such that users can search work requests.  
BR 4.1  
The system shall allow the Company A corporate intranet authorized user community to create work requests in the system.  
FR 6.9.8  
The Requestor module shall consist of sections containing the following types of information:  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure  
FR 6.10.1  
The system will be able to indicate a purchase unit of measure, which can be different from the consumption unit of measure.  
BR 6.1  
The system shall be capable of integrating with Oracle Purchasing application for the generation of vendor records, and purchase orders, as well as the receipt of materials, and viewing of purchase order balances.  
FR 6.10.6  
The system will be able to associate multiple addresses for each vendor record.  
BR 6.5  
The system shall have the capability to generate and track purchase orders approved from requisitions.  
ITPD-38444 GFR-001  
BR 6.5  
The system shall have the capability to generate and track purchase orders approved from requisitions.  
ITPD-38444 GFR-002  
The interface processes Purchase Order transmissions and delivers the packets to INFOR.  
BR 6.6  
The system shall have the capability to perform receipt transactions  
ITPD-38444 GFR-003  
The interface processes Parts and Service Receipts transmissions and delivers the packets to Oracle EBS.  
BR 6.7  
The system shall have the capability to track invoice information and reconcile expenditures against purchase orders/receipts.  
 ITPD-38444 GFR-003  
The interface processes Parts and Service Receipts transmissions and delivers the packets to Oracle EBS.  
BR 5.15  
The system shall have the capability to reorder parts based on stocking parameters  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 REQ-001  
Each Requisition is processed as a unique data set.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 REQ-002  
The Requisition either passes all Fusion/Oracle validation and then is passed to EBS or it is returned to INFOR, via email, as an exception.  
BR 6.1  
The system shall be capable of integrating with Oracle Purchasing application for the generation of vendor records, and purchase orders, as well as the receipt of materials, and viewing of purchase order balances.  
ITPD-38444 REQ-003  
The Requisition can be for parts and/or Service.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 PO-001  
Each PO Line is transmitted in a separate file that is part of a unique data set.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 REC-001  
Each Receipt is a unique data set.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 REC-002  
The Receipt either passes all Fusion/Oracle validation and then is passed to EBS or it is returned to INFOR, via email, as an exception.  
BR 6.1  
The system shall be capable of integrating with Oracle Purchasing application for the generation of vendor records, and purchase orders, as well as the receipt of materials, and viewing of purchase order balances.  
ITPD-38444 REC-003  
The Receipt can be for Parts or Service.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 CCD-001  
Cost Code Data is transmitted from EBS as a unique data set.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 CCD-002  
Cost Code Data transmissions contain add and change transaction types.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 ED-001  
Employee Data is transmitted from Oracle HR as a unique data set.  
BR 6.2  
The system shall have the capability to exchange pertinent procurement data with Oracle iProcure.  
ITPD-38444 ED-002  
Employee Data transmissions contain add and change transaction types.  
BR 7.3  
The system shall provide authorized users with the ability to extract/export data from the system in an acceptable format such as Microsoft Excel.  
BR 4.7  
The system shall be able to modify/control equipment information based on user permissions.  
BR 3.12  
The system shall be able to identify equipment records as instruments requiring calibration.  
FR 6.3.11  
The system provides a checkbox identifying the record as an instrument on all equipment screens.  
BR 3.13  
The system shall be able to capture the status of an instrument.  
FR 6.3.12  
The system provides a definable status field on the Equipment record.  
BR 3.14  
The system shall be able to identify the classification of an instrument.  
FR 6.3.13  
The system provides a class field on the Equipment Record View tab for classification purposes.  
BR 3.15  
The system shall be able to store calibration data including calibration limits, ranges, units of measure, tolerances, test points, comments and standards used at an instrument level (Calibration Information).  
FR 6.3.14  
The system provides for creating and storing calibration data by instrument or instrument category including calibration limits, ranges, units of measure, tolerances, test points, comments, and standards.  
BR 3.16  
The system shall be able to designate differing units of measure for inputs vs. outputs in calibration testing.  
FR 6.3.15  
The system provides separate units of measure for a test point and test point output.  
BR 3.17  
The system shall be able to designate differing units of measure for individual test points within a set of test points on an instrument.  
FR 6.3.16  
The system provides a specific unit of measure for each test point on the instrument.  
BR 3.18  
The system shall provide a mechanism for storing calibration information as a template for like instruments.   
FR 6.3.17  
The system provides a Category code with calibration and test point data that can then be assigned to like instruments.  
BR 3.19  
The system shall be able to update calibration information as a batch for like instruments.  
FR 6.3.18  
The system provides an Update Equipment function in the Categories program to update all equipment assigned to that category.  
BR 3.20  
The system shall provide a mechanism for updating an instrument to a Measurement Device.  
FR 6.3.19  
The system provides a field to update equipment as a Measurement Device on the Equipment screen.  
BR 3.21  
The system shall be able to track the location of an instrument and shall maintain a history of all location changes.  
FR 6.3.20  
The system provides for a location in the Equipment structure that creates a history record in the Events tab each time the equipment location is changed.  
BR 3.22  
The system shall be able to track the parent system of an instrument and shall maintain a history of all equipment hierarchy changes.  
FR 6.3.21  
The system provides an equipment hierarchy on the Equipment Structure tab and captures hierarchy changes on the Events tab.  
BR 3.23  
The system shall provide a method of tracking calibration standards as serialized equipment and as standardized inventory items.  
FR 6.3.22  
The system provides for tracking of serialized equipment marked as calibration standards through the Part screen in the Record View tab.  
BR 3.24  
The system shall have the ability to identify all calibration work performed with a given standard within a given time frame. (Reverse Traceability)  
FR 6.3.23  
The system provides for reverse traceability for a defined date range using a defined standard.  
BR 3.25  
The system shall provide a mechanism for performing a criticality risk assessment on an instrument and capturing the results.  
FR 6.3.24  
The system provides a method of performing a criticality assessment on an instrument based on a predefined set of questions.  
BR 3.26  
The system shall provide a mechanism for identifying the criticality of an instrument.  
FR 6.3.25  
The system provides a Classification field with business rule capability to define the criticality of an instrument.  
BR 3.27  
The system shall provide a mechanism for attaching scanned documentation to an instrument record.  
FR 6.3.26  
The system provides for scanned document attachment capability on Equipment records on the Documents tab.  
BR 3.28  
The system shall provide a mechanism for communicating test point level instructions/comments and transferring this information to calibration work orders.  
FR 6.3.27  
The system provides a comments field on each calibration test point that can be used for instructions/comments and will transfer to the calibration work order.  
BR 3.29  
The system shall have a mechanism for tracking the approval flow of the CRA Process outside of the instrument record (CRA Request)  
FR 6.3.28  
The Instrument CRA screen is used to track the approval of an instrument update.  
BR 3.30  
The CRA Request mechanism shall include designation of Criticality Risk Assessment, Interval of calibration, range and tolerance information.  
FR 6.3.29  
A CRA request process is provided to document the criticality classification, the interval of calibration, the range, and the tolerance of the instrument. A check box on the instrument will indicate the CRA has been completed.  
BR 3.31  
The system shall provide automatic updates of the Category field and updating the CRA assessment results into the appropriate equipment Category field.  
FR 6.3.30  
The system provides capabilities through FLEX SQL configuration to update information on the equipment form based on the CRA assessment.  
BR 3.32  
The system shall allow for the association of instruments to parts records.  
FR 6.3.31  
The system provides for the direct association of instruments to part records on the Equipment Record View tab in the Part Information section.  
BR 3.33  
The system shall provide a mechanism for identifying an instrument as missing.  
FR 6.3.32  
The system provides a means to mark an instrument as 'missing' by creating and using a defined supplemental status on the Record View tab.  
BR 4.12  
The system shall allow authorized users to generate calibration work orders from a preventive maintenance schedule.  
FR 6.4.27  
The system provides authorized users a Generate WO program to generate PM work orders by work order type - 'PMCAL - Calibration' work orders.  
BR 4.13  
The system shall be able to associate multiple PM schedules to an individual instrument.  
FR 6.4.28  
The system allows multiple PM schedules to be associated to one instrument on the PM Schedules tab.  
BR 4.14  
The system shall allow authorized users to generate calibration work orders for unscheduled or on-demand calibrations.  
FR 6.4.29  
The system allows for the creation of unscheduled calibration work orders in the Work Order program.  
BR 4.15  
The system shall provide a method of differentiating Calibration Work orders from general maintenance work orders.  
FR 6.4.30  
The system provides a way to categorize work orders by using a UDF checkbox labeled as 'Calibration WO' on the Work Order Record View tab.  
BR 4.16  
The system shall provide a method of differentiating calibration work orders performed by Company A technicians vs. performed by vendor calibration technicians.   
FR 6.4.31  
The system provides a 'Supplier' field on the Record View of the work order that can house the calibration vendor code.  
BR 4.17  
The system shall provide a mechanism for capturing the name of the vendor performing the calibration.  
FR 6.4.32  
The system provides a Supplier field on the work order that can indicate the calibration vendor.  
BR 4.18  
The system shall be able to identify which instruments have been sent off-site to external vendors.  
FR 6.4.33  
The system provides a work order status field that will designate that the calibration work order has been sent to a vendor. (Status = "With Vendor")  
BR 4.19  
The system shall provide a mechanism for vendor performed calibrations allowing users to attach scanned certificates.  
FR 6.4.34  
The system provides Document Attachment capability so that vendor certificates may be attached to a calibration record.  
BR 4.20  
The system shall be able to capture calibration data and status per test point for As-Found conditions and As-Left conditions including failures and adjustments during the calibration process.  
FR 6.4.35  
The system provides the ability to capture calibration data and status per test point for As-Found conditions and As-Left conditions including failures and adjustments during the calibration process.  
BR 4.21  
The system shall be able to capture the overall calibration status of an instrument As-Found at the time of the calibration and As-Left after all test points have been completed including failures and adjustments.  
FR 6.4.36  
The system provides the ability to capture the overall calibration status of an instrument As-Found at the time of the calibration and As-Left after all test points have been completed including failures and adjustments.  
BR 4.22  
The calibration technician must be able to see whether the entered calibration result is within or outside of the Calibration tolerance and the Adjustment tolerance.  
FR 6.4.37  
The system provides the means for the calibration technician to view whether the entered calibration results are within or outside of the Calibration tolerance on the calibration work order.  
BR 4.23  
The system shall provide a mechanism for capturing all standards used during the calibration of an instrument.  
FR 6.4.38  
The system provides the ability to capture the Standard used on a calibration work order.  
BR 4.24  
The system shall provide a method of verifying a standard is not past its expiration date before being used for calibration.  
FR 6.4.39  
The system provides business rules to identify standards past their expiration dates.  
BR 4.25  
The system must provide a work order status flow for the calibration work order.  
FR 6.4.40  
The system provides a work order status flow for the calibration work order.  
BR 4.26  
The calibration status shall exist independently of the work order status for the calibration work order.  
FR 6.4.41  
The system provides a calibration status that is independent of the work order status.  
BR 4.27  
The system shall provide a mechanism for documenting adjustments made during the performance of the calibration.  
FR 6.4.42  
The system provides As-Left information, test point comments and work order comments for calibration notes.  
BR 4.28  
The system shall provide a method for documenting out of tolerance "RAR" reference record from supporting systems for failed calibrations on critical equipment for calibrations requiring an RAR. This field will require population for work orders requiring an RAR.  
FR 6.4.43  
The system shall provide a field on the work order for capturing RAR Information (Trackwise #). Population of this field will be required via FLEX configuration for work orders requiring an RAR.   
BR 4.29  
The system shall be able to capture the employee performing a calibration work order.  
FR 6.4.44  
The system captures the e-Signature of the employee completing the work order.  
BR 4.30  
The system shall be able to capture the time required to perform a calibration work order.  
FR 6.4.45  
The system provides an "Hours Worked" field on the work order which captures the time worked by employee.  
BR 4.31  
The system shall provide a searchable database of unscheduled or scheduled calibration work order records.  
FR 6.4.46  
The system provides a searchable database of work orders. Calibration work orders will have a checkbox to identify calibration work orders whether they are scheduled or unscheduled.  
BR 4.32  
The system shall provide a method of associating a calibration work order to a repair work order resulting from the performance of calibration activities.  
FR 6.4.47  
The system provides a Parent/Child relationship with regard to Work Orders which can associate repair work orders to calibration work orders.  
BR 4.33  
The system shall allow for a grace period for the performance of a calibration work order after the work order is generated. This grace period is determined procedurally based on criticality and frequency of calibration.  
FR 6.4.48  
The system provides a PM Due Date and PM Interval that defines the 'grace period' for each Calibration PM schedule.  
BR 4.34  
The system shall provide the capability of tracking schedule extensions for calibration work orders.  
FR 6.4.49  
The system provides a work order status field that will designate that the calibration is working its way through the extension process.  
BR 4.35  
The system shall provide a method of identifying instruments having 3 or more sequential calibrations found out of tolerance.  
FR 6.4.50  
The system provides reporting to identify instruments that have 3 or more consecutive failures.  
BR 4.36  
The system shall provide a method of displaying work instructions on a calibration work order.  
FR 6.4.51  
The system provides comments text blocks for work instructions.  
BR 4.37  
The system shall provide a method of indicating whether an instrument passed or failed calibration at the calibration work order level.  
FR 6.4.52  
The system provides a calibration status to indicate whether the instrument passed or failed calibration.  
BR 4.38  
The system shall provide a method of identifying a corrective work order as a calibration work order.  
FR 6.4.53  
The system provides a checkbox indicating the work order includes calibration information.  
BR 4.39  
The system shall provide a mechanism for identifying different sets of test points for a particular category/instrument.  
FR 6.4.54  
The system provides 'sets' at the test point level to separate groups of test points on scheduled calibrations.  
BR 4.40  
The system provides automated e-mail notification of equipment owner for out of tolerance calibration results upon completion of supervisor review of the order. If the equipment owner is not populated, no notification will be sent.  
FR 6.4.55  
The system provides an email notification tool that can be configured to send email notifications for out of tolerance calibrations.  
BR 5.17  
The system shall provide a mechanism for identifying a part as a Calibration Standard.  
FR 6.5.21  
The system provides a checkbox on the Part record that is linked to the Equipment which identifies the part as a Calibration Standard.  
BR 7.6  
The system shall provide access to historical calibration event records in a searchable format within the framework of the application.  
FR 6.11.6  
The system provides a historical calibration event for each equipment record on the Events tab of Equipment.  
BR 7.7  
The system shall provide access to historical calibration related records maintaining the relationship to the equipment/instrument record for migrated equipment.  
FR 6.11.7  
The system will provide an additional tab linked to equipment records to show historical calibration data that occurred outside of CMMS.  
BR 7.12  
The system shall provide a method of displaying all active or open calibration work orders.  
FR 6.11.12  
The system will provide a list of all active calibration work orders based on the work order type, Calibration WO checkbox, and Status.  
BR 7.15  
The system shall provide a method of displaying all historical calibrations performed on an instrument.  
FR 6.11.15  
The system provides event history of all calibrations performed on an instrument.  
BR 11.4  
The System shall provide a method of storing and accessing legacy system transactional data that will not be migrated into the base application.  
FR 6.12.4  
The system will provide access to legacy system transactional data searchable by instrument through a customized data grid.  
BR 11.5  
Legacy information shall be accessible for migrated instruments and equipment as well as obsolete, non-migrated instruments and equipment.  
FR 6.12.5  
This should be: The system will provide access to legacy system information via an equipment tab custom data grid for currently installed equipment and a custom transactional data grid for equipment that may or may not be in Infor 10.  
BR 11.6  
Legacy information shall be sortable, searchable, filterable, and exportable.  
FR 6.12.6  
Legacy transactional data will be located in a custom data grid which will be sortable, searchable, filterable and exportable to Excel.  
BR 3.34  
The system shall provide a means to store meter readings for equipment/instrument.  
FR 6.3.33  
The system provides a meter tab to record PI meter readings both automatically and manually. The tab will provide options to update and track meter readings for each specific equipment/instrument.  
BR 4.41  
The system shall provide a means to generate work orders based on meter reading.  
FR 6.4.56  
The system provides a Meter-based PM schedule to generate PM work orders based on meter readings from the PI system.  
BR 4.42  
The system shall provide a means to pull specific readings from the PI System.  
FR 6.4.57  
The system provides a “Meter” tab on equipment and a “PI Alert Data” screen to extract reading points from the PI System.  
BR 4.43  
The system shall provide a means to store alert critical and extreme limits for equipment/instrument.  
FR 6.4.58  
The system provides the “Aspects” tab on the Monitored Equipment screen to setup min/max values for alert critical and extreme limits for non-metered equipment/instrument. For metered equipment, the limits are set on the record view of the equipment screen.  
BR 4.44  
The system shall provide means to generate automated e-mail notification based on equipment alert criticals and extremes.  
FR 6.4.59  
The system provides a place to setup automated e-mail notification when equipment alert critical/extremes are met or surpassed. Automated email notification is handled through the existing “Alert Management” menu, using the “E-mail Alerts” tab.  
BR 4.45  
The system shall provide means to generate work orders based on equipment alert extremes.  
FR 6.4.60  
The system provides a mechanism to generate work orders if extremes are met or surpassed. Work order generation is handled through the existing “Alert Management” menu, using the “Work Order Alerts” tab.  
BR 10.2  
The system shall provide the ability to interface with the PI System.  
FR 6.9.9  
The system provides the “PI Meter Equipment” grid, Equipment “Meter” tab and “PI Alert Data” grid displaying instruments associated with PI tags and the related data.  
BR 3.35  
The system shall provide a mechanism for performing a system impact assessment (SIA) on equipment and capturing the results.  
FR 6.3.34  
The system provides a method of performing an SIA on equipment based on a predefined set of questions.  
BR 3.36  
The system shall provide a mechanism for identifying the latest SIA performed on equipment.  
FR 6.3.35  
The system provides a field on the equipment record that shows the latest CRA/SIA request.  
BR 3.38  
The system shall provide a method to update multiple equipment on one CRA/SIA request.  
FR 6.3.37  
The system provides an extra tab on the latest CRA/SIA Request screen to allow input of additional equipment on one request.  
BR 3.39  
The system shall provide a method to roll-down updates to the children of an equipment using the CRA/SIA Request screen.  
BR 3.39  
The system shall provide a method to roll-down updates to the children of an equipment using the CRA/SIA Request screen.  
FR 6.3.52  
The system has the ability to determine the ‘Direct Impact or Child of Direct Impact’ status on a piece of equipment and roll-down to their children (if any), on the Equipment CRA/SIA Request screen.  
BR 3.39  
The system shall provide a method to roll-down updates to the children of an equipment using the CRA/SIA Request screen.  
FR 6.3.53  
The system provides SIA request types on the Equipment CRA/SIA Request screen that will determine the SIA on a piece of equipment and roll-down to their children (if any) that are functional systems.  
BR 6.8  
The system shall allow users to manually change the status of purchase orders within CMMS.  
FR 6.10.7  
The system will allow authorized user groups to update the status of a purchase order manually.  
BR 6.9  
The system shall allow all sites to order parts and in multiple currencies.  
FR 6.10.8  
Authorized users from all sites have the ability to create a purchase requisition and set the currency that is not specific to the organization.  
BR 6.10  
The system should allow for proper pricing to be transferred to the purchase order for all units of measures.  
FR 6.10.9  
The part record on a purchase order shall maintain the same quantity, price, and unit of measure as the purchase requisition it was generated from.  
BR 10.3  
The system shall maintain updated active supplier information for suppliers that accept orders from Oracle EBS.  
FR 6.9.10  
The system will provide the ability to perform batch updates to the Supplier screen with active supplier data from Oracle EBS.  
BR 3.11  
The system shall provide a means to assess equipment for its criticality to business operations through the Reliability Ranking module.   
FR 6.3.39  
The system will provide a means to assess the Reliability Ranking of the equipment to determine the critical nature of the equipment in terms of business operations.  
BR 3.40  
The system shall be able to identify reviewers for revisions to preventive maintenance entities.  
FR 6.3.40  
The system will provide reviewer fields on PM Entity screens for users to select the primary approvers for revisions.  
BR 3.41  
The system shall be able to identify the reasoning for revisions to preventative maintenance entities.  
FR 6.3.41  
The system will provide a free text field on PM Entity screens to enter the reason for revisions.  
BR 3.42  
The system shall be able to put restrictions on initiators being approvers for GMP PM entity revisions with the exclusion of administrative changes.  
FR 6.3.42  
The system will provide a means to restrict initiators from approving GMP PM Entity revisions that are not administrative changes.  
BR 3.43  
The system shall be able to put the enforcement of QA Review for GMP PM Entity revisions with the exclusion of administrative changes.  
FR 6.3.43  
The system will provide a means to enforce QA Review on GMP PM Entity revisions that are not administrative changes.  
BR 3.44  
The system shall be able to consolidate multiple processes for equipment onboarding.  
FR 6.3.44  
The system will provide the Equipment Onboarding screen that incorporates equipment creation, CRA/SIA, Reliability Ranking, PM assessment, Alarm Classification, and optional upload.  
BR 3.45  
The system shall provide a process to install or retire equipment  
FR 6.3.45  
The system will provide the Equipment Install/Retire Request screen to install or retire equipment.  
BR 3.46  
The system shall be able to by-pass QA Review on non-GMP Equipment CRA/SIA Requests for equipment in the TD, RESEARCH, and CAM GEF departments.  
FR 6.3.46  
The system will provide a means to by-pass QA review for certain equipment on Equipment CRA/SIA Request   
BR 3.47  
The system shall be able to by-pass review on calibration work orders that does not contain critical in the classification.  
FR 6.3.47  
The system will provide a means to by-pass review and go straight to close status on scheduled and unscheduled calibration work orders.  
BR 4.46  
The system shall be able to by-pass planning when creating an unscheduled work order.  
FR 6.4.61  
The system will provide a means to by-pass PLNSCH review (Planning) and go straight to Released status when creating unscheduled work orders.  
BR 3.48  
The system shall provide a means to automatically update equipment information on PM Schedules when the equipment is being updated.  
FR 6.3.48  
The system will provide a flex that will update fields on the Equipment tab of the PM Schedules screen after updating fields on the Equipment screen.  
BR 4.47  
The system shall be able to enforce a requirement to populate a value in the Supervisor field for DEN and SOL work orders.  
FR 6.4.62  
The system will provide a flex that will make the Supervisor field a mandatory requirement for DEN and SOL work orders when the WO is saved to the Released, Review, and Closed Statuses.  
BR 3.49  
The system shall be able to hide the “Assigned To” field on PM Schedules and Equipment screens.  
FR 6.3.49  
The system will be able to hide the “Assigned To” field in the PM Schedule and Equipment screen.  
BR 3.50  
The system shall be able to detect if a PM Entity is GMP or Non-GMP, based on the status of the related equipment.  
FR 6.3.50  
The system shall be able to detect if a PM Entity is GMP or Non-GMP from the status of the related equipment which determines the selection of approvals lists for PM Entity revisions.  
BR 7.17  
The system shall provide a means to lookup open revisions on PM Entities.  
FR 6.11.17  
The system will provide a grid showing all active open revisions on PM Schedules, Job Plans. Material Lists, and Routes.  
BR 4.49  
The system shall allow authorized users to use checklists to track work performed on work orders.  
FR 6.4.64  
The system will be able to display the correct completion status of the checklist on a work order, when any type of checklist is used.  
BR 3.51  
The system shall provide a mechanism to assess the classification of alarm records and create alarm records.  
FR 6.3.54  
The system provides an “Alarm Classification” screen which can be used to create alarm records and perform an alarm classification assessment.  
BR 3.52  
The system shall provide a means to show alarm records with alarm classification values.  
FR 6.3.55  
The system provides an “Alarms” screen which displays alarm records with alarm classification values.  
BR 3.53  
The system shall provide a means to upload Alarm Classification requests.  
FR 6.3.56  
The system provides a means to upload Alarm Classification data for the respective request/multiple requests at a time.  
BR 10.4  
The system shall maintain an outbound Equipment publication service.  
FR 6.9.2  
The system will publish records indicating changes to Equipment master attributes for select Equipment to a database staging table, for external systems to read.  
BR 10.4  
The system shall maintain an outbound Equipment publication service.  
FR 6.9.3  
The system will query for PM or PMCAL Work Orders that are Overdue each day at midnight Organization time. The system will then publish an Overdue status for select Equipment that are impacted to a database staging table, for external systems to read. Overdue status is defined as an open Work Order not equal to 3RVW, 3QA, 3UPD, and Due Date less than the date at the location of the Equipment on the Work Order.  
BR 10.4  
The system shall maintain an outbound Equipment publication service.  
FR 6.9.13  
The system will determine if no other Overdue maintenance exists against an Equipment or its Child Equipment, once a PM or PMCAL Work Order completes for an Equipment deemed Overdue. If it finds none, the system will publish a Not Overdue status for select Equipment, as well as for any select Parent Equipment that have no other Child Equipment in an Overdue status, to a database staging table, for external systems to read. Completed status is defined as when the Work Order reaches a status of 3RVW, 3QA, 3UPD or a system status of C. Overdue status is defined as having an open PM or PMCAL Work Order against the Equipment not equal to 3RVW, 3QA, 3UPD, and Due Date less than the date at the location of the Equipment.  
BR 10.4  
The system shall maintain an outbound Equipment publication service.  
FR 6.9.14  
The system will determine if an Equipment structure change causes any Equipment to become Overdue or Not Overdue. Overdue status rolls up to all Parent Equipment. Not Overdue status rolls up to all Parent Equipment with no other Overdue Child Equipment. The system will publish an Overdue or Not Overdue status for select Equipment to a database staging table, for external systems to read. Overdue status is defined as having an open PM or PMCAL Work Order against the Equipment not equal to 3RVW, 3QA, 3UPD, and Due Date less than the date at the location of the Equipment.  
BR 10.4  
The system shall maintain an outbound Equipment publication service.  
FR 6.9.15  
A “Broadcast Changes” checkbox, editable by Administrator User Groups, will be available on the Equipment screen to select Equipment for which status and Equipment master attribute changes will be recorded onto a database staging table, for external systems to read.  
BR 10.5  
The system shall provide the ability to interface with the Advanced Scheduler application.  
FR 6.9.16  
Database Views will be installed to stage data for the Advanced Scheduler application to pull. The Views will display general Work Order data for select Work Orders, Trades associated with Activities on each Work Order, sum of Estimated Hours of each Trade per Work Order, and sum total of all Estimated Hours per Work Order.  
BR 3.54  
Protected “PM Due” and “PMCAL Due” indicators will be made available on the Equipment screen to indicate whether an Equipment is Overdue for Preventative Maintenance or Calibration, respectively.  
FR 6.3.63  
Protected “PM Due” and “PMCAL Due” checkboxes will be added to the Equipment screen as indicators of Preventative Maintenance or Calibration Overdue status of corresponding Equipment. Overdue status is defined as having an open PM or PMCAL Work Order against the Equipment not equal to 3RVW, 3QA, 3UPD, and Due Date less than the date at the location of the Equipment.  
BR 3.55  
The system shall allow change in to be completed for different areas or zones of manufacturing at different times.  
FR 6.3.64  
BOE will allow Equipment to be categorized by Zone and Area.  
BR 3.56  
The system shall be able to store process settings of the equipment.  
FR 6.1.18  
A settings tab on Equipment records will detail existing attribute settings relevant to the Equipment record.  
BR 3.57  
The system shall be able to route and track revisions to the BOE and attributes.  
FR 6.1.19  
BOE will be revision controlled and support a review status prior to approval.  
BR 3.58  
The system shall be able to record the reasoning for revisions to BOEs or equipment attributes.  
FR 6.3.65  
Revision Reason field will capture justification for revision.  
BR 3.59  
The system shall support the ability to perform bulk data uploads of Attributes, BOE Equipment and BOE Settings.  
FR 6.3.66  
The CMMS Import Utility application will support bulk data upload for BOE, attributes, and attribute settings.  
BR 3.60  
The system shall display whether each piece of equipment selected for a campaign is dormant or is currently due for PM.  
FR 6.1.13  
The system enables authorized users to generate Bill of Equipment records detailing lists of Equipment validated for use in manufacturing a specific product and the status of the Equipment; as well as to associate the Equipment on the BOE with the attribute settings required by the BOE.  
BR 3.61  
All current process settings for a piece of equipment shall be able to be viewed.  
FR 6.1.14  
A settings tab on Equipment records will detail existing attribute settings relevant to the Equipment record.  
BR 3.62  
A record of initial process settings shall be able to be viewed in the change request.  
FR 6.3.67  
IEL will include a tab detailing a comparison between initial (Equipment) settings and BOE settings.  
BR 3.63  
A record of date and time of implementation of new process settings shall be able to be viewed in the Equipment Change Summary report.  
FR 6.3.68  
The IEL will provide a timestamp for new process settings that have been implemented.  
BR 3.64  
The system shall allow a user to change process settings on a piece of equipment outside of campaign changeover.  
FR 6.3.69  
A settings tab on Equipment records will detail existing attribute settings relevant to the Equipment record.  
BR 4.51  
The system shall compare the current process settings of each piece of equipment selected in the IEL with the incoming process settings for the new campaign.  
FR 6.4.68  
A settings comparison tab is available on the Equipment Change Request screen.  
BR 4.52  
The system shall generate work orders to change any current process settings which differ from the incoming campaign’s process settings.  
FR 6.4.69  
The system will generate a Work Order for each Zone under the Equipment Change Request. The system will also generate Routine Maintenace Work Orders against each Equipment on the IEL, as children to the respective Zone Work Orders. The Routine Maintenance Work Orders will include checklists to change any current process settings which differ from the incoming campaign’s process settings; and will be organized into Activities on the Work Order. corresponding to the Trade of the respective settings being changed.  
BR 4.53  
The system shall generate work orders to change any current process settings to N/A in cases where those attributes are not specified for the incoming campaign.  
FR 6.4.70  
If the Equipment Change Request does not specify the value for a process setting that exists on an Equipment included in the IEL, then the ECR will include work orders to change the value of those unspecified settings to N/A on the Equipment record.  
BR 4.54  
The system shall not generate work orders in cases where the current equipment process setting matches that of the incoming campaign.  
FR 6.4.71  
Equipment Change Requests will not generate Work Orders to change process settings when the value of the setting on the Equipment included in the IEL matches that setting value on the BOE.  
BR 4.55  
A single work order shall be generated for each piece of equipment for each trade and zone, with a checklist of attributes to be updated. The checklist notes shall be pre-populated with the new value and old value.  
FR 6.4.72  
Upon approval of the Equipment Change Request, a single work order shall be generated for each piece of equipment for each trade and zone, with a checklist of attributes to be updated per the associated BOE. The checklist notes shall be pre-populated with the new value and old values.  
BR 4.56  
System shall provide the ability to complete WO based on checked process setting status.  
FR 6.4.73  
The system automatically updates Equipment attributes when respective checklist items are marked as successfully completed. Otherwise the system does not update the Equipment.  
BR 4.57  
System shall provide the ability to complete WO based on unchecked process setting status.  
FR 6.4.73  
The system automatically updates Equipment attributes when respective checklist items are marked as successfully completed. Otherwise the system does not update the Equipment.  
BR 4.58  
The system will assign Work Orders to the trade that is assigned to the associated parameters (BOE Settings).  
FR 6.4.74  
BOE will support association of attribute settings with specific trades against which the Work Orders to update the attributes will be generated.  
  
End of general requirements.  
  
Start of requirements regarding reports/reporting:  
  
BR 7.2  
The system shall provide standard reports, as well as the ability for a user to create and save searches.  
FR 6.1.7  
CMMS built-in Cognos reporting functionality will be used for reporting.  
BR 7.5  
The system shall allow for auto generated reports to be distributed via email  
BR 7.8  
The system shall provide a report to access historical calibration measurement data records.  
FR 6.11.8  
The system provides a Calibration History report which shows historical calibrations on each piece of equipment specified.  
BR 7.9  
The system shall provide a Calibration Work Order Report capturing a calibration event.  
FR 6.11.9  
The system will provide a custom Calibration Work Order report that reports all calibration data for the specified equipment/instrument.  
BR 7.10  
The system shall provide a Confirmation of Calibration report displaying the last calibration performed on an instrument.  
FR 6.11.10  
The system will provide a custom Confirmation of Calibration report that displays the last calibration performed on an instrument by Organization code.  
BR 7.11  
The system shall provide a method of displaying all parents and/or children records for an instrument. (Hierarchy Report)  
FR 6.11.11  
The system provides a report for equipment structure to show parent/child relationships.  
BR 7.13  
The system shall provide a report to forecast scheduled calibrations including calibration data.  
FR 6.11.13  
The system provides a method of forecasting scheduled calibrations including calibration data:  
BR 7.14  
The system shall provide a report displaying all devices calibrated using a specific standard over a specified period of time. (Reverse Traceability)  
FR 6.11.14  
The system provides a reverse traceability feature by tying a part record, marked as a standard, to an instrument.  
BR 7.16  
The system shall provide a method of printing calibration labels using the existing report functionality.  
FR 6.11.16  
The system provides a method to print calibration labels using the built in Cognos reporting functions. The report will be able to be generated automatically or manually.   
BR 7.18  
A summary change report shall be generated with Current equipment settings and BOE settings.  
FR 6.11.19  
An Equipment Change Summary report shall be generated with Current equipment settings and BOE settings.  
BR 7.19  
An BOE Summary Report that will show BOE header information, BOE equipment and BOE Settings.  
FR 6.11.20  
A BOE Summary Report will show BOE header information, BOE equipment and BOE Settings.  
BR 7.20  
An Revision Change Detail Report for BOEs will show changes between revisions from the record view, BOE equipment, and BOE equipment Settings  
FR 6.11.21  
An Revision Change Detail Report for BOEs will show changes between revisions from the record view, BOE equipment, and BOE equipment Settings  
BR 7.21  
An Equipment Change Summary Report that shows IEL record view information, incoming equipment list with calibration overdue status and dormancy information,settings comparison to the BOE, excecutable wokrorder info , inital process settings , and esigniture section.  
FR 6.11.22  
An Equipment Change Summary Report will show IEL record view information, incoming equipment list with calibration overdue status and dormancy information,settings comparison to the BOE, excecutable wokrorder info , inital process settings , and esigniture section.  
BR 4.50  
The system shall provide authorized users a method to generate and review audit trail reports of work orders.  
FR 6.4.65  
The system will be able to pass records of changes made to information on the screen of a work order of any type to an attached ‘Audit Trail Review’ tab. The system will then compile and display the records in an audit trail report in the ‘Audit Trail Review’ tab.  
  
End of reporting requirements.  
  
Start of Regulatory requirements:  
  
UR-REG-01  
The system must have appropriate controls to (a) protect the system and records from inadvertent as well as deliberate destruction or alteration and (b) prevent, detect, and mitigate harmful effects of viruses, worms, and other harmful codes and ensure their accurate and ready retrieval throughout the records retention period. (§11.10c, Annex 11 7.1, MHRA Data Retention section; EU Vol 4 Chpt 4 4.1 and 4.10; EU Annex 11 7.1; PMDA MHLW Ord 169 Article 9 1; EMA Q10, PDA Data Integrity Code of Conduct 3.3.1.2)  
FS-REG-01  
ITCD-22525, Information Security Policy provides a control mechanism to protect Company A systems from inadvertent and deliberate destruction and harmful effects of harmful codes and programs. PRCD-94210, Global Records Retention and Disposition Policy outlines a methodology to protect and retain system data and ensure accurate retrieval of data throughout the retention period.  
UR-REG-02  
The system must be able to display or print accurate and complete copies of records suitable for inspection. Raw data must permit the full reconstruction of the activities resulting in the generation of the data.  (§11.10b, Annex 11 8.1, MHRA Raw Data section; PDA Data Integrity Code of Conduct 3.3.1.5)  
FS-REG-02  
The system shall display or print all documents suitable for use during an inspection.  
The system provides a viewable audit trail which covers user interaction, system records at the workflow level.  
The audit trail can be generated from the Audit Trail Review tab.   
UR-REG-03  
The system must produce reports of electronically stored data, including audit trails. (Annex 11 8.1, MHRA Raw Data section; PDA Data Integrity Code of Conduct 3.3.1.5)  
FS-REG-03  
System shall generate and store data in the form of reports including audit trails.  Reports can be generated from the report section.  
UR-REG-04  
Where required, the system must use operational checks to enforce permitted sequencing of Step(s) and events. (§11.10f)  
FS-REG-04  
The system provides the workflow functionality which will have a sequence of review, approve, release and complete statuses.  Workflow will promote to the next status only after the approval in a sequential manner.  
UR-REG-05  
The system must incorporate built-in checks where appropriate in order to determine the validity of source of data input or operational instruction. (§11.10h, Annex 11 5)  
UR-REG-06  
The system should employ additional checks for critical data entered manually to ensure the accuracy of the data.  This check may be done by a second operator step or by validated electronic means.  (§11.10 f, Annex 11 6, MHRA Raw Data section; PDA Code of Conduct 3.3.4)  
FS-REG-06  
Approver will view and make the decision whether to approver or reject. After all the approver signoff, workflow will be promoted to the next status.  
UR-REG-07  
The system must automatically log users off after a specified period of inactivity. (§11.10d, g, Annex 11 12.1, MHRA Computerized System User Access section)  
FS-REG-07  
Upon inactivity, the system shall automatically log users out after a configured period of inactivity.  
UR-REG-08  
Open systems must employ digital signatures and data encryption as necessary in order to maintain data authenticity, integrity, and confidentiality. (§11.30, Annex 11 7.1, 12.1, MHRA Data Section)  
UR-REG-09  
The system must provide human readable forms of signed electronic records (e.g., computer screen displays, printouts).  These should bear the printed name of the signer, the date and time of the signing, and the meaning of the signature (e.g., review, approval, responsibility, and authorship). (§11.50, Annex 11 14, MHRA Data Integrity)  
FS-REG-09  
The system shall capture the following information with all electronic signatures:  
•  The unique username for the user.  
•  The date and time that the signature was captured, stored and displayed with CMMS Application Server time.  
•  The meaning of the signature is inherent in the record that the signature is stamped on.  
UR-REG-10  
The system must provide a permanent link between signatures (whether electronic or handwritten) executed to electronic records and their associated electronic records to ensure that signatures cannot be excised, copied, or transferred to falsify an electronic record by normal functionality and user authorization. (§11.70, Annex 11 14, MHRA Data Integrity)  
FS-REG-10  
Network ID’s are permanently linked to records in the Audit Trail.  Access is assigned according to PRCD-15979, Company A Account Management Procedure.  
Access to the application will be granted based on the users Network ID and AD group membership.  
The requirements are also supported through adherence to SOP PRCD-30916, IT Controls: Security Management.  
In the event of an upgrade or migration, this data will remain in the Audit Trail linked to Company A Network ID.  
UR-REG-11  
The system must be backed up and all relevant data/records must be retained and retrievable.  Backups must be complete and accurate data/records.  (§11.10c, Annex 11 7.2, MHRA Data Retention and Backup sections; EMA Q10 )  
FS-REG-11  
This requirement is supported by ITPD-82011, Backup and Restore Requirements and Test Plan.  
UR-REG-12  
The system must use secure data retention storage locations to prevent data from being saved to unauthorized file storage locations including removable devices. (§11.10c, Annex 11 7.1, MHRA Data Retention section; PDA Data Integrity Code of Conduct 3.3.1.4)  
FS-REG-12  
CMMS data will be retained within the validated system databases.  Access to the system data is controlled according to CMMS Application Management PRCD-16000.    
CMMS servers are within a secure data center on Company A network location which adheres to global data integrity requirements.  
UR-REG-13  
If the system is used for archiving data, the system must lock archived records such that they cannot be altered or deleted without detection and audit trail.  The archive arrangements must be designed to permit recovery and readability of the data and metadata.  
UR-REG-14  
The system must employ controls that maintain unique ID/password combinations such that no two individuals have the same combination of ID and Password. The system should not allow IDs to be reassigned or deleted once an ID is affixed to an electronic record.  The system should allow for the ID to be deactivated. (§11.10d, §11.100a, §11.300a, Annex 11 12.1, MHRA Data Section)  
FS-REG-14  
User accounts are controlled using Active Directory, which follows the company standard security controls as per PRCD-30916, IT Controls: Security Management and guidelines established in ITCD-36476, Password Policy.  
If a user is deactivated from the network, the system will not allow the user to access the application.  The CMMS audit trail will retain the electronic records containing the user’s information and will not be deleted.  
UR-REG-15  
The system must incorporate periodic mandatory expiration of passwords or other access keys. (§11.300b, §11.10d, Annex 11 12.1)  
FS-REG-15  
User accounts are controlled using Active Directory, which follows the company standard password policy as per ITCD-36476, Password Policy.  
UR-REG-16  
For systems that use non-biometric electronic signature, it must employ at least two distinct identification components such as identification code and password. (§11.10a, Annex 11 12.1, MHRA Data Section)  
FS-REG-16  
The system will use active directory login credentials, and thus will be compliant with Company A password policy ITCD-36476, Password Policy.  
UR-REG-17  
The system must use technical means to administer non-biometric electronic signatures to ensure that improper attempted use by anyone other than the genuine owner requires collaboration of two or more individuals. (§11.200a, Annex 11 12.1, MHRA Computerized System User Access section)  
FS-REG-17  
System has the ability to differentiate the electronic signature between signing off at the approval step and restricts approval access based on user groups and does not permit a user to approve a stage of the workflow if the user group is not configured to approval privilege.  
User accounts are controlled using Active Directory, which follows the company user management policy as per SOP PRCD-15979, Company A Account Management Procedure and PRCD-30916 “IT Controls: Security Management”.  
UR-REG-18  
The system must allow electronic signatures to be permanently linked to their respective record and include the time and date that there were applied and demonstrate the means to retain the link between the signature and the record, e.g., in situations when the data in a system is being migrated due to upgrade or retirement. (§11.70, Annex 11 14, MHRA Data section)  
FS-REG-18  
The system shall directly associate all signatures to the electronic record that the signature signs.  
Signatures are applied to the entities assigned to (i.e; PM Revision, Work Order Status Change).  
UR-REG-19  
The system must require at least two individual-specific electronic signature components for the initial signing when signings are performed within a single, continuous period.  Subsequent signings must be executed using at least one electronic signature component that is only executable by, and designed to be used only by, the individual. (§11.200a, MHRA Computer System Transactions Section)  
FS-REG-19  
System Access requirement is fulfilled through adherence to SOP PRCD-15979, Company A Account Management Procedure and PRCD-30916, IT Controls: Security Management for granting access.  
UR-REG-20  
The system must employ the same controls for electronic signatures as it does for electronic records and must include them as part of any human readable form of the electronic record (such as electronic display or printout). (§11.50b, Annex 11 8.1, MHRA Data section, MHRA Raw Data section; PDA Data Integrity Code of Conduct 3.3.1.5)  
FS-REG-20  
Signatures bear the user ID, printed name of the signer, the date and time of the signing, and the meaning of the signature.   
The electronic signatures Are displayed when applicable on validated reports (i.e; work order report).   
UR-REG-21  
When a computerized system is used for recording certification and batch release, the system must allow only Qualified Persons to certify the release of the batches and it should clearly identify and record the person releasing or certifying the batches. This should be performed using an electronic signature.  (Annex 11 15)  
UR-REG-22  
The system must have logical controls to restrict access and system functionality, and use to authorize individuals based on job responsibilities or roles. (§11.10d, g, Annex 11 12.1, MHRA Computerized System User Access section)  
FS-REG-22  
System will support restricting access to authorize individuals based on job responsibilities through creation of different Groups. Users will request access to AD groups through BAM and system will synchronize users in AD groups automatically.  
The system shall allow access groups to be defined, which control the functionality in the system that associated users are permitted to use.  
UR-REG-23  
The system must limit access to authorized individuals by using unique user ID/password login, or equivalent biometric identifier. (§11.10d, 11.200a, 11.300a, Annex 11 12.1, MHRA Computerized System User Access section)  
FS-REG-23  
System will support restricting access to authorize individuals based on job responsibilities through creation of different AD Groups.  
System Access requirement is fulfilled through adherence to SOP PRCD-15979, Company A Account Management Procedure for granting access.  
The system is integrated with the Active Directory, which also follows the company security policy which includes unique user ID / password logins.  
UR-REG-24  
The system must support individual user accounts/access, including unique logins for system administrators, to allow actions in the audit trail(s) to be attributed to a specific individual. (§11.10d, 2.1, MHRA Computerized System User Access section)  
FS-REG-24  
System will incorporate audit trails with changes not obscuring previously recorded information.  
UR-REG-25  
The system must allow administrator to assign appropriate privileges to each user account. (§11.10d, Annex 11 12.1)  
FS-REG-25  
The application shall allow access groups to be defined, which control the functionality in the application that associated users are permitted to use.  
The application shall allow Administrator users to associate a user account with a single access group, thereby defining the functionality that the user can execute.  
UR-REG-26  
The system must not allow write access for shared, groups, guests (or similar) accounts.  (§11.10d, MHRA Computerized System User Access section)  
FS-REG-26  
The application shall allow access groups to be defined which grants ‘read-only’ access only to specified functional areas of the application.  
UR-REG-27  
The system must demonstrate access levels granted to users and historical information regarding user access level and track any changes to system-specific accounts, privileges, and roles in the system. (§11.10d , Annex 11 12.1, MHRA Computerized System User Access section)  
FS-REG-27  
The system access is granted by assigning different users an AD Group.  
The access management will be performed using BAM, which will record details of access requests and approvals.  
Any changes to user or group access levels and historical information will be maintained in the Audit Trail.  
UR-REG-28  
The system must have the ability to configure system administrator rights (permitting activities such as data deletion, database amendment or systems configuration changes) to limit functionality.  Administrator rights to not be combined with roles/functionality that can be assigned to individuals with a direct interest in the data (data generation, data review or approval). (MHRA Computerized System User Access section)  
FS-REG-28  
System administrator (Admin) role will not be assigned to individuals with direct interest in the data.  
The Administrator role (Company A System Admin) is specifically for those who will make changes to system.  
UR-REG-29  
The system must have documented transaction safeguards/monitoring alerts in place to immediately detect any attempts at unauthorized use of IDs and/or passwords and to report such attempts to the appropriate system security personnel or organization/site management. (§11.300d, Annex 11 12.1)  
FS-REG-29  
System will support LDAP integration on for login and hence this requirement is fulfilled through adherence to SOP ITCD-22525, IT Information Security Policy and PRCD-30916, IT Controls: Security Management.  
Account lockout/notification upon incorrect entry of username and password are handled via active directory when the user attempts to access the system server.  
Upon successive invalid login attempts, the user account is locked per company policy.  
UR-REG-30  
If the system utilizes devices such as tokens or cards that bear or generate ID or password information, the devices must function properly and prevent alteration in an unauthorized manner. (§11.300e, Annex 11 12.1)  
UR-REG-31  
For systems that incorporate the use of biometric signatures, mechanisms must be employed to ensure that biometric signatures cannot be used by anyone other than the individual whose biometric profile matches that on file. (§11.200b, Annex 11 12.1, MHRA Computerized System User Access section)  
UR-REG-32  
If the system is a data acquisition system, it must have secure access to prevent unauthorized changes to electronic data.  (MHRA Computerized System User Access section; PDA Code of Conduct 3.4.1)  
UR-REG-33  
The system must incorporate and maintain audit trails which record all relevant changes and deletions, with changes not obscuring previously recorded information, including changes executed by the system administrator.  The reason for the change or deletion must be documented.  The system must be able to generate printouts of the audit trail. (§11.10e, Annex 11 8.2, 9, MHRA Audit Trail section; EMA Q8, Q15, MHRA Raw Data Section)  
FS-REG-33  
System shall be able to incorporate and maintain the audit trail record related to changes and deletions made in the system with changes not obscuring previously recorded information, including changes executed by the system administrator.   
System must have the electronic proof stating the reason for the deletion and system must be able to print the audit trail document.  
UR-REG-34  
The system audit trail must provide secure (not editable), date and time-stamped record of the action (obtained from a secure, reliable source, i.e. the server and not the client PC) and the identity of the operator any time an electronic record is created, modified, or deleted. (§11.10e, Annex 11 8.2, 9, 12.4, MHRA Audit Trail section; PDA Data Integrity Code of Conduct 3.3.1.3)  
FS-REG-34  
System shall have the ability to generate a secure audit trail report of the actin from application server which must provide the time stamp information’s in non-editable format when an particular action is performed. The report generated from the system is non-editable.  
UR-REG-35  
The system must not allow users to amend or switch off the audit trail. (§11.10e, Annex 11 9, MHRA Audit Trail Section)  
FS-REG-35  
System provides an audit trail on events within the system.  
System will generate and store audit trails based on the time zone generated by the CMMS application server.  
The Audit Trail is configured by the System Admin.  Any deactivation to Audit Trail fields are managed under IT Change Control.  
UR-REG-36  
The system must record the creation, change, and cancellation of access authorizations. (§11.300d, Annex 11 12.3, MHRA Data Section).  
FS-REG-36  
System provides an audit trail on events within the system.  
System will generate and store audit trails based on the time zone generated by the CMMS application server.  
The Audit Trail is configured by the System Admin.  Any deactivation to Audit Trail fields are managed under IT Change Control.  
  
End of Regulatory requirements.