Contains Nonbinding Recommendations

Computer Software Assurance for Production and Quality Management System Software

---

Guidance for Industry and Food and Drug Administration Staff

Document issued on February 3, 2026.

This document supersedes "Computer Software Assurance for Production and Quality System Software," issued September 24, 2025.

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 800-835-4709 or 240-402-8010, or by email at industry.biologics@fda.hhs.gov.

U.S. FOOD & DRUG ADMINISTRATION

U.S. Department of Health and Human Services
Food and Drug Administration
Center for Devices and Radiological Health
Center for Biologics Evaluation and Research

GRZAN

Preface

Public Comment

You may submit electronic comments and suggestions at any time for Agency consideration 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 20852-1740. Identify all comments with the docket number FDA-2022-D-0795. Comments may not be acted upon by the Agency until the document is next revised or updated.

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 GUI00017045 and complete title of the guidance in the request.

CBER

Additional copies are available from the Office of Communication, Outreach, and Development (OCOD), Center for Biologics Evaluation and Research (CBER), by calling 800-835-4709 or 240-402-8010, by email, industry.biologics@fda.hhs.gov, or from the Internet at https://www.fda.gov/vaccines-blood-biologics/guidance-compliance-regulatory-information-biologics/biologics-guidances.

GRZAN

Table of Contents

I. Introduction 1
II. Background 2
III. Scope 4
IV. Definitions 4
V. Computer Software Assurance 5
A. Computer Software Assurance Risk Framework 6
(1) Identifying the Intended Use 6
(2) Determining the Risk-Based Approach 8
(3) Production or Quality Management System Software Changes 11
(4) Determining the Appropriate Assurance Activities 12
(5) Additional Considerations for Assurance Activities 14
(6) Establishing the Appropriate Record 17
B. Considerations for Electronic Records Requirements 21
Appendix A. Examples 23
Example 1: Nonconformance Management System 23
Example 2: Learning Management System (LMS) 27
Example 3: Business Intelligence Applications 30
Example 4: Software as a Service (SaaS) Product Life Cycle Management System (PLM) . 34

Computer Software Assurance for Production and Quality Management System Software

---

Guidance for Industry and Food and Drug Administration Staff

This guidance represents the current thinking of the Food and Drug Administration (FDA or Agency) on this topic. It does not establish any rights for any person and is not binding on FDA or the public. You can use an alternative approach if it satisfies the requirements of the applicable statutes and regulations. To discuss an alternative approach, contact the FDA staff or Office responsible for this guidance as listed on the title page.

I. Introduction[1]

FDA is issuing this guidance to provide recommendations on computer software assurance for computers and automated data processing systems used as part of medical device production or the quality management system. This guidance:

- Describes "computer software assurance" as a risk-based approach to establish confidence in the automation used for production or quality management systems, and identifies where additional rigor may be appropriate; and
- Describes various methods and testing activities that may be applied to establish computer software assurance and provide objective evidence to fulfill regulatory requirements, such as computer software validation requirements in quality management system obligations, including requirements in 21 CFR Part 820, which includes

[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 Inspections and Investigations (OII).

incorporations by reference of the 2016 edition of ISO 13485[2] (hereafter referred to as "Part 820").[3]

This guidance supplements FDA's guidance, "General Principles of Software Validation" (hereafter referred to as the "Software Validation guidance") except this guidance supersedes Section 6: Validation of Automated Process Equipment and Quality System Software of the Software Validation guidance.

For the current edition of the FDA-recognized consensus standard referenced in this document, see the FDA Recognized Consensus Standards Database.[4]

In general, FDA's guidance documents do not establish legally enforceable responsibilities. Instead, guidances describe the Agency's current thinking on a topic and should be viewed only as recommendations, unless specific regulatory or statutory requirements are cited. The use of the word *should* in Agency guidances means that something is suggested or recommended, but not required.

II. Background

FDA envisions a future state where the medical device ecosystem is inherently focused on device features and manufacturing practices that promote product quality and patient safety. FDA has sought to identify and promote successful manufacturing practices and help device manufacturers raise their manufacturing quality level. In doing so, one goal is to help manufacturers produce high-quality medical devices that align with the laws and regulations implemented by FDA. Compliance with quality management system obligations including those in Part 820 is required for manufacturers of finished medical devices to the extent they engage in operations to which those obligations apply. Quality management system obligations include requirements for medical device manufacturers to develop, conduct, control, and monitor production processes to ensure that a device conforms to its specifications,[5] including requirements for manufacturers to validate computer software used as part of production or the

[2] All references to ISO 13485 in this guidance are to ISO 13485:2016, Medical devices — Quality management systems — Requirements for regulatory purposes.

[3] On February 2, 2024, FDA issued a final rule amending the device Quality System Regulation, 21 CFR Part 820, to align more closely with international consensus standards for devices (89 FR 7496, available at https://www.federalregister.gov/d/2024-01709). This final rule took effect on February 2, 2026. This rule removed the majority of the current requirements in Part 820, including 21 CFR 820.70, and instead incorporates by reference the 2016 edition of the International Organization for Standardization (ISO) 13485, Medical devices - Quality management systems – Requirements for regulatory purposes, in Part 820. As stated in the final rule, the requirements in ISO 13485 are, when taken in totality, substantially similar to the requirements of the current Part 820, providing a similar level of assurance in a firm's quality management system and ability to consistently manufacture devices that are safe and effective and otherwise in compliance with the Federal Food, Drug, and Cosmetic Act (FD&C Act).

[4] Available at https://www.accessdata.fda.gov/scripts/cdrh/cfdocs/cfStandards/search.cfm

[5] See Subclause 7.5 of ISO 13485.

quality management system for its intended use.[6,7] The recommendations on computer software assurance in this guidance are intended to promote product quality and patient safety, and correlate to higher-quality outcomes. This guidance addresses practices relating to computers and automated data processing systems used as part of production or the quality management system.

In recent years, advances in manufacturing technologies, including the adoption of automation, robotics, simulation, and other digital capabilities, have allowed manufacturers to reduce sources of error, optimize resources, and reduce patient risk. FDA recognizes the potential for these technologies to provide significant benefits for enhancing the quality, availability, and safety of medical devices, and has undertaken several efforts to help foster the adoption and use of such technologies.

Specifically, FDA has engaged with stakeholders via the Medical Device Innovation Consortium (MDIC), site visits to medical device manufacturers, and benchmarking efforts with other industries (e.g., automotive, consumer electronics) to keep abreast of the latest technologies and to better understand stakeholders' challenges and opportunities for further advancement. As part of these ongoing efforts, medical device manufacturers have expressed a desire for greater clarity regarding the Agency's expectations for software validation for computers and automated data processing systems used as part of production or the quality management system. Given the rapidly changing nature of software, manufacturers have also expressed a desire for a more iterative, agile approach for validation of computer software used as part of production or the quality management system.

Traditionally, software validation has often been accomplished via software testing and other verification activities conducted at each stage of the software development life cycle. However, as explained in FDA's Software Validation guidance, software testing alone is often insufficient to establish confidence that the software is fit for its intended use. Instead, the Software Validation guidance recommends that "software quality assurance" focus on preventing the introduction of defects into the software development process, and it encourages use of a risk-based approach for establishing confidence that software is fit for its intended use.

FDA believes that applying a risk-based approach to computer software used as part of production or the quality management system would better focus manufacturers' quality assurance activities to help ensure product quality while helping to fulfill validation requirements. For these reasons, FDA is providing recommendations on computer software assurance for computers and automated data processing systems used as part of medical device production or the quality management system. FDA believes that these recommendations will help foster the adoption and use of innovative technologies that promote patient access to high-quality medical devices and help manufacturers to keep pace with the dynamic, rapidly changing technology landscape, while promoting compliance with laws and regulations implemented by FDA.

---

[6] See Subclauses 4.1.6, 7.5.6, and 7.6 of ISO 13485.

[7] This guidance discusses the "intended use" of computer software used as part of production or the quality management system (see Subclauses 4.1.6 and 7.5.6 of ISO 13485), which is different from the intended use of the device itself (see 21 CFR 801.4).

III. Scope

This guidance provides recommendations regarding computer software assurance for computers or automated data processing systems used as part of production or the quality management system for medical devices.

This guidance is not intended to provide a complete description of all software validation principles. FDA has previously outlined principles for software validation, including managing changes as part of the software life cycle, in FDA's Software Validation guidance. This guidance applies the risk-based approach to software validation discussed in the Software Validation guidance to production or quality management system software. This guidance additionally discusses specific risk considerations, acceptable testing methods, and efficient generation of objective evidence for production or quality management system software through the life cycle of the medical device.

This guidance does not provide recommendations for the design and development verification or validation requirements for device software functions, which are software functions that meet the definition of a device under section 201(h) of the Federal Food, Drug, and Cosmetic Act (FD&C Act). For more information regarding FDA's recommendations for the validation of medical device software, see the Software Validation guidance.

IV. Definitions

The following definitions apply for the purposes of this guidance.[8]

Cloud Computing (Cloud): Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model is composed of five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. The cloud is composed of three service models: software as a service (SaaS), platform as a service (PaaS), and infrastructure as a service (IaaS). The cloud model is also composed of four deployment models: private cloud, community cloud, public cloud, and hybrid cloud.[9]

Infrastructure as a service (IaaS): The capability provided to the consumer is to provision processing, storage, networks, and other fundamental computing resources where the consumer is able to deploy and run arbitrary software, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, and deployed applications; and possibly limited

[8] Some of the definitions originate from other FDA sources (e.g., Software Validation guidance) and are applicable in those instances.

[9] This definition is derived from the National Institute of Standards and Technology's "The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology," available at https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

control of select networking components (e.g., host firewalls).[10]

Platform as a service (PaaS): The capability provided to the consumer is to deploy onto the cloud infrastructure consumer-created or acquired applications created using programming languages, libraries, services, and tools supported by the provider.[11] The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage, but has control over the deployed applications and possibly configuration settings for the application-hosting environment.[12]

Software as a service (SaaS): The capability provided to the consumer is to use the provider's applications running on a cloud infrastructure. The applications are accessible from various client devices through either a thin client interface, such as a web browser (e.g., email), or a program interface. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, storage, or even individual application capabilities, with the possible exception of limited user-specific application configuration settings.[13]

V. Computer Software Assurance

Computer software assurance is a risk-based approach for establishing and maintaining confidence that software is fit for its intended use. This approach considers the risk of compromised safety and/or quality of the device (should the software fail to perform as intended) to determine the level of assurance effort and activities appropriate to establish confidence in the software. Because the computer software assurance effort is risk-based, it follows a least-burdensome approach, where the burden of validation is no more than necessary to address the risk. Such an approach supports the efficient use of resources, in turn promoting product quality.

In addition, computer software assurance establishes and maintains that the software used in production or the quality management system is in a state of control throughout its life cycle ("validated state"). This is important because manufacturers increasingly rely on computers and automated processing systems to monitor and operate production, alert responsible personnel, and transfer and analyze production data, among other uses. By allowing manufacturers to leverage principles such as risk-based testing, unscripted testing, continuous performance monitoring, and data monitoring, as well as validation activities performed by other entities (e.g., developers, suppliers, cloud service providers), the computer software assurance approach provides flexibility and agility in helping to provide assurance that the software maintains a validated state consistent with applicable quality management system obligations.

Software that is fit for its intended use and that maintains a validated state should perform as intended, helping to ensure that finished devices will be safe and effective and in compliance with regulatory requirements (see 21 CFR 820.1(a)(1)). Section V outlines a risk-based

[10] Id.
[11] This capability does not necessarily preclude the use of compatible programming languages, libraries, services, and tools from other sources.
[12] See footnote 9.
[13] Id.

framework for computer software assurance.

A. Computer Software Assurance Risk Framework

The following approach is intended to help manufacturers establish a risk-based framework for computer software assurance throughout the software's life cycle. The approach outlined can be applied, but is not limited, to automation tools (e.g., BOTS or automatic workflows), data analytic tools, artificial intelligence/machine learning tools, and cloud computing when used as part of production or the quality management system.[14]

Examples of applying this risk framework to various computer software assurance situations are provided in Appendix A.

(1) Identifying the Intended Use

The regulation requires manufacturers to validate software **that is used as part of production or the quality management system** for its intended use (see Subclauses 4.1.6, 7.5.6, and 7.6 of ISO 13485). This includes various cloud computing models related to computerized systems, such as IaaS, PaaS, and SaaS.

To determine whether the requirement for validation applies, manufacturers must determine whether the software is or will be used as part of production or the quality management system (whether directly or to support production or the quality management system).

Software with the following intended uses is considered to be used **directly** as part of production or the quality management system:

- Software intended for automating production processes, inspection, testing, or the collection and processing of production data; and
- Software intended for automating quality management system processes, collection and processing of quality management system data, or maintaining a quality record established under applicable quality management system obligations.

Software with the following intended uses is considered to be used to **support** production or the quality management system:

- Software intended for use as development tools that test or monitor software systems or that automate testing activities for the software used as part of production or the quality management system, such as those used for developing and running scripts or software embedded in the production equipment (e.g., firmware); and
- Software intended for automating general record-keeping for production or the quality management system that is not part of the quality record.

Both kinds of software are used as part of production or the quality management system and

[14] Cloud computing used as part of production or the quality management system, including when supporting associated recordkeeping and manufacturing activities, is within the scope of this guidance. Cloud computing used as part of device software functions are not in the scope of this guidance.

must be validated under Subclauses 4.1.6, 7.5.6, or 7.6 of ISO 13485 as appropriate. However, as further discussed below, supporting software often carries lower risk, such that under a risk-based computer software assurance approach, the effort of validation may be reduced accordingly without compromising safety.

On the other hand, software with the following intended uses generally **is not** considered to be used as part of production or the quality management system, such that the requirements for validation in Subclauses 4.1.6, 7.5.6, and 7.6 of ISO 13485 would not apply:

- Software intended for management of general business processes or operations not specific to production or the quality management system, such as email or accounting applications; and
- Software intended for establishing or supporting infrastructure not specific to production or the quality management system, such as networking, user authentication, or continuity of operations (e.g., backup and restore).

FDA recommends manufacturers focus on the intended use of the software when considering cloud computing models, as not all cloud computing models are "directly" used as part of production or the quality management system. For example, an IaaS cloud storage solution falls into the category of infrastructure, but may be used to store quality records established under applicable quality management system obligations, in which case the IaaS cloud storage solution would be considered to be used directly as part of production or the quality management system. In this example, FDA recommends manufacturers focus the assurance effort on the features or functions relevant to the integrity of the records and 21 CFR Part 11 requirements applicable to the records intended to be stored.

Conversely, an IaaS cloud storage solution may support infrastructure to store production and process data; this would not be considered an established quality management system record. In this example, the IaaS cloud storage solution does not support production or the quality management system, and the requirements for validation in Subclauses 4.1.6, 7.5.6, and 7.6 of ISO 13485 would not apply. When storage of data in the cloud is independent of whether or not the data is part of the quality record, it is the manufacturer's obligation to determine what the appropriate level of risk is for that application. Manufacturers may consider a least-burdensome approach to assuring the IaaS cloud storage solution is adequate for their business.

As described in Subclauses 4.1.6, 7.5.6, and 7.6 of ISO 13485, the specific approach and activities associated with software validation and revalidation are required to be proportionate to the risk associated with the use of the software, including the effect on the ability of the product to conform to specifications. FDA recognizes that software used in production or the quality management system is often complex and comprised of multiple features, functions, and operations;[15] software may have one or more intended uses depending on the individual features, functions, and operations of that software. In cases where the individual features, functions, and operations of the software have different roles within production or the quality management

[15] 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.

system, they may present different risks with different levels of validation effort. FDA recommends that manufacturers examine the intended uses of the individual features, functions, and operations to facilitate development of a risk-based assurance strategy. Manufacturers may decide to conduct different assurance activities for individual features, functions, or operations as related to the intended use.

For example, a commercial off-the-shelf (COTS) spreadsheet software may be comprised of various functions with different intended uses. When utilizing the basic input functions of the COTS spreadsheet software for an intended use of documenting the time and temperature readings for a curing process, a manufacturer may not need to perform additional assurance activities beyond those conducted by the COTS software developer and initial installation and configuration. The intended use of the software, "documenting readings," only supports maintaining a record of the process information and poses a low process risk. As such, initial activities such as the successful vendor assessment and software installation and configuration may be sufficient to establish that the software is fit for its intended use and maintains a validated state. However, if a manufacturer also utilizes built-in functions of the COTS spreadsheet to create custom formulas that are directly used in production or the quality management system, then additional risks and data integrity considerations may be present. For example, if a custom formula automatically calculates time and temperature statistics to monitor the performance and suitability of the curing process, then additional validation by the manufacturer might be necessary.

For the purposes of this guidance, we describe and recommend a computer software assurance framework where manufacturers examine the intended uses of the individual features, functions, or operations of the software. However, in simple cases where software has only one intended use (e.g., if all of the features, functions, and operations within the software share the same intended use), manufacturers may not find it helpful to examine each feature, function, and operation individually. In such cases, manufacturers may develop a risk-based approach and consider assurance activities based on the intended use of the software overall.

FDA recommends that manufacturers document their decision-making process for determining whether a software feature, function, or operation is or will be used as part of production or the quality management system.

(2) Determining the Risk-Based Approach

Once a manufacturer has determined that a software feature, function, or operation is or will be used as part of production or the quality management system, a risk-based analysis is used to determine appropriate assurance activities. It should be noted that in accordance with Subclause 4.1.2 of ISO 13485, a manufacturer is required to apply a risk-based approach to the control of the appropriate processes needed for the quality management system. Broadly, this risk-based approach entails systematically identifying reasonably foreseeable software failures, determining whether such a failure poses a high process risk, and systematically selecting and performing assurance activities commensurate with the medical device or process risk, as applicable. Manufacturers should select an appropriate frequency for performing assurance activities based on their risk-based analysis and accounting for their processes and procedures, as appropriate for

the software and assurance activities being performed.

Note that conducting a risk-based analysis for computer software assurance for production or quality management system software, as described in this guidance, is distinct from performing a risk analysis for a medical device as described in the International Organization for Standardization (ISO) 14971:2019 – *Medical devices – Application of risk management to medical devices*. The risk-based analysis for production or quality management system software focuses on those factors that may impact or prevent the software from performing as intended, such as proper system configuration and management, security of the system, data integrity, data storage, data transfer, or operation error. A risk-based analysis for production or quality management system software should consider which failures are reasonably foreseeable (as opposed to likely) and the risks resulting from each such failure. For example, in a risk-based analysis a manufacturer may consider the risks resulting from a power outage, which may not be likely to occur but is reasonably foreseeable to occur over the life cycle of a production or quality management system. This guidance discusses both *process risks* and *medical device risks*. A process risk refers to the potential to compromise production or the quality management system. A medical device risk refers to the potential for a device to harm the patient or user. When discussing medical device risks, this guidance focuses on the medical device risk resulting from a quality problem that compromises safety.

Specifically, FDA considers a software feature, function, or operation to pose a high **process** risk **when its failure to perform as intended may result in a quality problem that foreseeably compromises safety, meaning a medical device risk**. This process risk identification step focuses only on the process, as opposed to the medical device risk posed to the patient or user. Examples of software features, functions, or operations that are generally **high process risk** are those that:

- Maintain process parameters (e.g., temperature, pressure, or humidity) that affect the physical properties of product or manufacturing processes that are identified as essential to device safety;
- Measure, inspect, analyze and/or determine acceptability of product or process with limited or no additional human awareness or review;
- Perform process corrections or adjustments of process parameters based on data monitoring or automated feedback from other process steps without additional human awareness or review;
- Produce instructions for use or other labeling provided to patients and users that are necessary for safe operation of the medical device; and/or
- Automate surveillance, trending, or tracking of data that the manufacturer identifies as essential to device safety (e.g., cybersecurity) and quality.

In contrast, FDA considers a software feature, function, or operation not to pose a high process risk **when its failure to perform as intended would not result in a quality problem that foreseeably compromises safety**. This includes situations **where failure to perform as intended would not result in a quality problem**, as well as situations **where failure to perform as intended may result in a quality problem that does not foreseeably lead to compromised safety**. Examples of software features, functions, or operations that generally are

not high process risk include those that:

- Collect and record data from the process for monitoring and review purposes that do not have a direct impact on production or process performance;
- Are used as part the quality management system for Corrective and Preventive Actions (CAPA) routing, automated logging/tracking of complaints, automated change control management, or automated procedure management;
- Are intended to manage data (process, store, and/or organize data), automate an existing calculation, increase process monitoring, or provide alerts relevant to managing data when an exception occurs in an established process; and/or
- Are used to support production or the quality management system, as explained in Section V.A.1 above.

FDA acknowledges that process risks associated with software used as part of production or the quality management system are on a spectrum, ranging from high process risk to low process risk. Manufacturers should determine the risk of each software feature, function, or operation as the risk falls on that spectrum, depending on the intended use of the software. FDA is primarily concerned with the review and assurance for those software features, functions, and operations that are high process risk because a failure also poses a medical device risk. For the purposes of this guidance, FDA is presenting the process risks in a binary manner, "high process risk" and "not high process risk." A manufacturer may still determine that a process risk is, for example, "moderate," "intermediate," or even "low" for purposes of determining assurance activities; in such a case, the portions of this guidance concerning "not high process risk" would apply. As discussed in Section V.A.4 below, assurance activities should be conducted for software that is "high process risk" commensurate with the medical device risk and "not high process risk" commensurate with the process risk.

Example: An Enterprise Resource Planning (ERP) Management system contains a feature that automates manufacturing material restocking. This feature automates material ordering and delivery to appropriate production operations. However, a qualified person checks the materials before their use in production. The failure of this feature to perform as intended may result in a mix-up in restocking and delivery, which would be a quality problem because the wrong materials would be restocked and delivered. However, the delivery of the wrong materials to the qualified person should result in the rejection of those materials before use in production; as such, the quality problem should not foreseeably lead to compromised safety. The manufacturer identifies this as an intermediate (not high) process risk and determines assurance activities commensurate with the process risk. The manufacturer has performed an evaluation of the ERP vendor, the ERP system information, and has configured the ERP system for its operations. The manufacturer implements any remaining assurance activities associated with the material order and delivery automation.

Example: A similar feature in another ERP management system performs the same tasks as in the previous example except that it also automates checking the materials before their use in production. A qualified person does not check the material first. The manufacturer identifies this as a high process risk because the failure of the feature to perform as intended may result in a quality problem that foreseeably compromises safety. As such, the manufacturer will determine

assurance activities that are commensurate with the related medical device risk. The manufacturer has previously performed assurance activities on the material identification data system, the automated material scanning systems (barcode scanners), evaluated the ERP vendor/information, and has configured the ERP system for their operations. The manufacturer implements any remaining assurance activities associated with the ordering and delivery automation.

Example: An ERP management system contains a feature to automate product delivery. The medical device risk depends upon, among other factors, the correct product being delivered to the device user. A failure of this feature to perform as intended may result in a delivery mix-up, which would be a quality problem that foreseeably compromises safety; as such, the manufacturer identifies this as a high process risk. Since the failure would compromise safety, the manufacturer will next determine the related increase in medical device risk and identify the assurance activities that are commensurate with the medical device risk. In this case, the manufacturer has not already implemented any of the identified assurance activities, so the manufacturer implements all of the assurance activities identified in the analysis.

Example: An automated graphical user interface (GUI) function in the production software is used for developing test scripts based on user interactions and to automate future testing of modifications to the user interface of a system used in production. A failure of this GUI function to perform as intended may result in implementation disruptions and software updates to the production system being delayed, but in this case, these errors should not foreseeably lead to compromised safety because the GUI function operates in a separate test environment. The manufacturer identifies this as a low (not high) process risk and determines assurance activities that are commensurate with the process risk. The manufacturer already undertakes some of those identified assurance activities so implements the remaining identified assurance activities.

(3) Production or Quality Management System Software Changes

For devices with approved premarket approval applications (PMA) or humanitarian device exemptions (HDE), PMA/HDE supplements are not required for changes to the manufacturing procedure or method of manufacturing that do not affect the safety or effectiveness of the device if they are reported to FDA in a periodic report (usually referred to as an annual report).[16] PMA/HDE supplements also are not required for modifications to manufacturing procedures or methods of manufacture that affect the safety and effectiveness of the device; these are submitted in a 30-day notice.[17] Changes to the manufacturing procedure or method of manufacturing may include changes to software used in production or the quality management system. For an addition or change to software used in production or the quality management system of devices with approved PMAs or HDEs, FDA recommends that manufacturers apply the principles outlined above in Section V.A.2 in determining whether the change may affect the safety or effectiveness of the device. In general, if a change may result in a quality problem that

[16] 21 CFR 814.39(b), 814.108, and 814.126(b)(1), and the "Annual Reports for Approved Premarket Approval Applications (PMA)" guidance.

[17] 21 CFR 814.39(f), 814.108, and 814.126(b)(1). Changes in manufacturing/sterilization site or to design or performance specifications do not qualify for a 30-day notice, see 21 CFR 814.39(a).

foreseeably compromises safety, then it should be submitted in a 30-day notice. If a change would not result in a quality problem that foreseeably compromises safety, then the change may be appropriate to report in an annual report.[18]

For example, a Manufacturing Execution System (MES) may be used to manage workflow, track progress, record data, and establish alerts or thresholds based on validated parameters, which are part of maintaining the quality management system. Failure of such an MES to perform as intended may disrupt operations but not affect the process parameters established to produce a safe and effective device. Changes affecting these MES operations are generally submitted in annual reports. In contrast, an MES used to automatically control and adjust established critical production parameters (e.g., temperature, pressure, process time) may be a change to a manufacturing procedure that affects the safety or effectiveness of the device. If so, changes affecting this specific operation would be submitted in a 30-day notice.

(4) Determining the Appropriate Assurance Activities

Once the manufacturer has determined whether a software feature, function, or operation poses a high process risk (a quality problem that may foreseeably compromise safety), the manufacturer should identify the assurance activities commensurate with the medical device risk or the process risk. In cases where the quality problem may foreseeably compromise safety (high process risk), the level of assurance should be commensurate with the medical device risk. In cases where the quality problem may not foreseeably compromise safety (not high process risk), the level of assurance rigor should be commensurate with the process risk. In either case, heightened risks of software features, functions, or operations generally entail greater rigor for assurance efforts (i.e., a greater amount of objective evidence). Conversely, relatively low risk (i.e., not high process risk) of compromised safety and/or quality generally entails less collection of objective evidence for the computer software assurance effort.

A software feature, function, or operation that could lead to severe harm to a patient or user would generally be high medical device risk. In contrast, a feature, function, or operation that would not foreseeably lead to severe harm would likely not be high medical device risk. In either case, the risk of the software's failure to perform as intended is commensurate with the resulting medical device risk.

If the manufacturer instead determined that the software feature, function, or operation does not pose a high process risk (i.e., it would not lead to a quality problem that foreseeably compromises safety), the manufacturer should consider the risk relative to the process (i.e., production or the quality management system). This is because the failure would not compromise safety, so the failure would not introduce additional medical device risk. For example, a function that collects and records process data for review would pose a lower process risk than a function that determines acceptability of product prior to human review.

[18] Manufacturers should also consult the "Enforcement Policy for Certain Supplements for Approved Premarket Approval (PMA) or Humanitarian Device Exemption (HDE) Submissions" guidance, which describes FDA's general recommendations for limited modifications to devices required to have an approved PMA or HDE to help address manufacturing limitations or supply chain disruptions.

Types of manual or automated testing that may be considered as part of the assurance activities commonly performed by manufacturers include, but are not limited to, the following:

- **Unscripted testing**: Dynamic testing in which the tester's actions are not prescribed by written instructions in a test case.[19] It includes:
    - Scenario Testing (Also referred to as Ad-Hoc Testing): A specification-based test case design technique based on exercising sequences of interactions between the test item and other systems.[20] (Users are considered to be other systems in this context.)
    - **Experience-based testing**: Class of test case design techniques based on using the experience of testers to generate test cases.[21] Experience-based testing can include concepts such as test attacks, tours, and error taxonomies which target potential problems such as security, performance, and other quality areas,[22] and can include:
        - **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. The relevant knowledge can be gained from personal experience, or can be encapsulated in, for example, a defects database or a "bug taxonomy."[23]
        - **Exploratory testing**: Experience-based testing in which the tester spontaneously designs and executes tests based on the tester's existing relevant knowledge, prior exploration of the test item (including results from previous tests), and heuristic "rules of thumb" regarding common software behaviors and types of failure. Exploratory testing looks for hidden properties, including hidden, unanticipated user behaviors, or accidental use situations that could interfere with other software properties being tested and could pose a risk of software failure.[24]
- **Scripted testing**: Testing in which test cases are recorded (e.g., document in a test management tool or in a spreadsheet) and can then be executed manually or executed automatically using an automated testing tool. The level of detail required for each test case and the evidence necessary to establish the software feature, function, or operation performs as intended depends on the risk posed by the software feature, function, or operation. For example, depending on the intended use, a more robust scripted testing where the test cases and evidence may include detailed requirements for repeatability, traceability, or auditability may be appropriate.

This guidance describes a risk-based approach manufacturers may consider in meeting regulatory requirements. It is not an exhaustive list of software testing methods and principles.

[19] IEC/IEEE/ISO 29119-1 Second edition 2022-01: Software and systems engineering – Software testing - Part 1: General Concepts, Section 3.133.
[20] Id. at Section 3.72.
[21] Id. at Section 3.36.
[22] Id. at Section 4.4.5.
[23] Id. at Section 3.32.
[24] See id. at Section 3.37.

FDA recognizes that there are software testing methods and approaches, beyond those referenced in the guidance, that manufacturers have the flexibility to consider and utilize, as appropriate.[25]

For example, the "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submission" guidance, which is applicable to devices with cybersecurity considerations and describes recommendations regarding the cybersecurity information to be submitted for devices under certain premarket submission types, includes recommendations for cybersecurity testing used to demonstrate the effectiveness of design and development activities. Manufacturers may consider utilizing the cybersecurity testing methods described in that guidance when conducting the assurance activities described in this guidance, as appropriate.

In general, FDA recommends that manufacturers apply principles of risk-based testing in which the management, selection, prioritization, and use of testing activities and resources are consciously based on corresponding types and levels of analyzed risk to determine the appropriate activities. For high process risk software features, functions, and operations, manufacturers may choose to consider more rigor such as the use of scripted testing or a hybrid approach of scripted testing and unscripted testing, scaled as appropriate, when determining their assurance activities. In contrast, for software features, functions, and operations that are not high process risk, manufacturers may consider using unscripted testing methods such as scenario testing, error-guessing, exploratory testing, or a combination of methods that is suitable for the risk. The testing examples discussed for high process risk and not high process risk are not exclusive to those categories. Manufacturers should apply the principles of risk-based testing to determine the appropriate type of testing to perform. For example, unscripted testing may be better suited to assure the software performs as intended even for high process risk features, functions, and operations. Conversely, a manufacturer may find it more effective and efficient to develop scripted testing and automate it for not high process risk features, functions, and operations.

(5) Additional Considerations for Assurance Activities

When deciding on the appropriate assurance activities, manufacturers should consider whether there are any additional controls or mechanisms in place throughout the quality management system that may decrease the impact of compromised safety and/or quality if failure of the software feature, function or operation were to occur. For example, as part of a comprehensive assurance approach, manufacturers can leverage the following to reduce the effort of additional assurance activities:

- Activities and established processes that provide control in production or fully verify processes in which software is involved. Such activities may include procedures to ensure integrity in the data supporting production, subsequent inspection or testing, or software quality assurance processes performed by other organizational units.

[25] For additional resources on current software testing methods and validation approaches, manufacturers may refer to various software standards and industry guidance, such as, but not limited to GAMP5 – A Risk-Based Approach to Compliant GxP Computerized Systems (Second Edition).

- Established purchasing control processes for selecting and monitoring software vendors. For example, the medical device manufacturer could incorporate the software development practices, validation work, and electronic information already performed by developers of the software as the starting point and determine what additional activities may be needed. For some lower-risk software features, functions, and operations, this may be all the assurance that is needed by the manufacturer.
- Additional process controls, including activities to reduce cybersecurity exposure,[26] that have been incorporated throughout production. For example, if a process is fully understood, all critical process parameters are monitored, and/or all outputs of a process undergo verification testing, these controls can serve as additional mechanisms to detect and correct the occurrence of quality problems that may occur if a software feature, function, or operation were to fail to perform as intended. In this example, the presence of these controls can be leveraged to reduce the effort of assurance activities appropriate for the software.
- The data and information periodically or continuously collected by the software for the purposes of monitoring or detecting issues and anomalies in the software after implementation of the software. The capability to monitor and detect performance issues or deviations and system errors may reduce the risk associated with a failure of the software to perform as intended and may be considered when deciding on assurance activities.
- The use of tools supporting software development and system life cycle activities (e.g., bug, anomaly tracking, requirement traceability tools) for the assurance of software used in production or as part of the quality management system whenever possible.
- The use of testing and results done in iterative cycles and continuously throughout the life cycle of the software used in production or as part of the quality management system.

FDA recognizes that manufacturers may have limited access to information from the software vendor as part of an assessment and recommends manufacturers establish and apply a risk-based analysis of the software vendor as part of their assurance approach. The manufacturer's assessment may consider various sources of information when deciding the appropriate level of control for the software vendor (e.g., purchasing controls). To evaluate the vendor's capabilities, whether cloud-based, on premise, or a hybrid, the manufacturer may consider activities including but not limited to:

- Onsite audits of the vendor, if applicable. FDA acknowledges that it may not be feasible or appropriate for a device manufacturer to audit the software vendor. Manufacturers may consider any alternative combination of information, as applicable, in a risk-based analysis of the controls and capabilities of the software vendor;
- Review of the vendor's accreditations and certifications (e.g., Service Organization Controls reports), and industry standard certifications (e.g., ISO certifications);
- Review of the vendor's practices and documentation for software development, software quality assurance, cybersecurity (e.g., security risk assessments, threat modeling, security

[26] See the "Cybersecurity in Medical Devices: Quality Management System Considerations and Content of Premarket Submission" guidance.

design and development reviews, software bill of materials (SBOM), and testing) and risk mitigation; and
- Review of the vendor's or software's data integrity capabilities or controls such as, but not limited to:
    - Retaining records, archiving data, and generating accurate and complete copies of records;
    - Securing data at rest and in transit (i.e., maintaining secure, computer-generated, time-stamped audit trails of users' actions and changes to data, encrypting data); and/or
    - Establishing and maintaining access controls, electronic signature controls and authorization checks for users' actions.

A manufacturer should establish and maintain within its procedures the requirements it has for suppliers on the basis of their ability to meet specified requirements and define the type and extent of control to be exercised over the product, services, and suppliers. Manufacturers should consider appropriate sources of information regarding the vendor in their evaluation decision. FDA recommends that manufacturers establish a risk-based approach to the evaluation of the vendor of software or service, the evaluation activities, and the appropriate objective evidence to retain.

For example, supporting software, as referenced in Section V.A.1, often carries lower risk, such that the assurance effort may generally be reduced accordingly. Because assurance activities used "directly" in production or the quality management system often inherently cover the performance of supporting software, assurance that this supporting software performs as intended may be sufficiently established by leveraging vendor evaluation and validation records, software installation, or software configuration, such that additional assurance activities (e.g., scripted or unscripted testing) may be unnecessary.

Example: A CAPA automation system is being written in Java script and a debugger tool is used to set up breakpoints and step through the code. Once the code is debugged, all the debugger content is removed prior to implementation. In this situation, the debugger tool is used to assist a software developer during the coding of a quality management system but is not subject to quality management system obligations because the COTS tool, which is not integrated with production or the quality management system, is not used as part of production or the quality management system. FDA recommends manufacturers establish a least-burdensome approach to ensure the tool performs as intended.

Example: A manufacturer is using a cloud storage solution for production data. The system has a network load specification, and a parameterization tool is used to simulate anticipated peak load of the production system. The load testing results shows objective evidence that the system can absorb the required user load and becomes part of the validation package. The parameterization tool is not the system of record of the testing result because it does not alter the code within the production system and the testing does not add any data to the production system. FDA recommends manufacturers establish a least-burdensome approach to ensure the tool performs as intended.

Manufacturers are responsible for determining the appropriate assurance activities for ensuring the software features, functions, or operations maintain a validated state. The assurance activities and considerations noted above are some possible ways of providing assurance and are not intended to be prescriptive or exhaustive. Manufacturers may leverage any of the activities, or a combination of activities, that are most appropriate for risk associated with the intended use.

(6) Establishing the Appropriate Record

When establishing the record, the manufacturer should capture sufficient objective evidence to demonstrate that the software feature, function, or operation was assessed and performs as intended. In general, FDA recommends the record include the following:

- The intended use of the software feature, function, or operation;
- The result of the risk-based analysis of the software feature, function, or operation; and
- Documentation of the assurance activities conducted, including:
    - A description of the testing conducted based on the assurance activity.
    - Issues found during testing (e.g., deviations, defects, and/or failures).
    - A conclusion statement declaring acceptability of the software for its intended use. If issues were found, FDA recommends including resolution of issues found as part of the conclusion statement. The manufacturer may consider including process controls implemented to address any impact from the issues to the intended use or appropriate risk justification addressing why the issues found will not impact the intended use.
    - Record of who performed testing/assessment and date the testing/assessment was performed.
    - Established review and approval when appropriate (e.g., when necessary, a signature and date of an individual with signatory authority).

Documentation of assurance activities need not include more evidence than necessary to show that the software feature, function, or operation performs as intended for the risk identified. FDA 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.[27]

Advances in digital technology may allow for manufacturers to leverage digital retention of results, automated traceability, automated testing, and electronic capture of work performed as objective evidence, reducing the need for manual or paper-based documentation. As a least-burdensome approach, **FDA recommends incorporating the use of digital records, such as system logs, audit trails, and other data generated and maintained by the software**, as opposed to paper documentation, screenshots, or duplicating results already digitally retained by the software when establishing the record associated with the assurance activities. When using digital records, FDA recommends manufacturers consider the intended use and the need for accuracy, reliability, integrity, availability, and authenticity of the record as part of the risk-based

[27] For the Quality Management System obligations for such records, including record retention period, see generally Subclause 4.2.5 of ISO 13485.

assurance approach established.

Table 1 provides some examples of ways to implement and develop the record when using the risk-based testing approaches, including testing approaches identified in Section V.A.4 above. Manufacturers may use alternative approaches and provide different documentation so long as their approach satisfies applicable legal documentation requirements.

Table 1 – Examples of Assurance Activities and Records

Assurance Activity	Test Plan	Test Results	Record (Including Digital)
Scripted Testing: Robust	• Test objectives • Test cases (step-by-step procedure) • Expected results • Independent review and approval of test plan when appropriate	• Result record obtained for each test case • Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Detailed report of testing performed • Result for each test case • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and the date the testing was performed • Established review and approval when appropriate
Scripted Testing: Limited	• Limited test cases (step-by-step procedure) identified • Expected results for the test cases • Identify unscripted testing applied • Independent review and approval of test plan when appropriate	• Result record obtained for each test case • Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Summary description of testing performed • Result for each test case • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate

Assurance Activity	Test Plan	Test Results	Record (Including Digital)
Unscripted Testing: Scenario Testing	• Testing of features and functions with no test plan	• Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Summary description of features and functions tested, and testing performed • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate
Unscripted Testing: Error guessing	• Testing of failure-modes with no test plan	• Details regarding any failures/ deviations found	• Intended use • Result of risk-based analysis • Summary description of failure-modes tested, and testing performed • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate

Assurance Activity	Test Plan	Test Results	Record (Including Digital)
Unscripted Testing: Exploratory Testing	• Establish high level test plan objectives with pass/fail criteria for each objective (no step-by-step procedure is necessary)	• Details regarding any failures/deviations found	• Intended use • Result of risk-based analysis • Summary description of the objectives tested, and testing performed • Issues found • Conclusion declaring acceptability of the software for its intended use, including the resolution or appropriate risk justification of issues found • Record of who performed testing and date the testing was performed • Established review and approval when appropriate

The following is an example of a record of assurance in a scenario where a manufacturer has developed a spreadsheet with the intended use of collecting and graphing nonconformance data stored in a controlled system for monitoring purposes. In this example, the manufacturer has established additional process controls and inspections that ensure non-conforming product is not released. In this case, failure of the spreadsheet to perform as intended would not result in a quality problem that foreseeably leads to compromised safety, so the spreadsheet would not pose a high process risk. The manufacturer conducted rapid exploratory testing of specific functions used in the spreadsheet to ensure that analyses can be created, read, updated, and/or deleted. During exploratory testing, all calculated fields updated correctly except for one deviation that occurred during the testing of the update. In this scenario, the record would be documented as follows:

- **Intended Use:** The spreadsheet is intended for use in collecting and graphing nonconformance data stored in a controlled system for monitoring purposes; as such, it is used as part of production or the quality management system. Because of this use, the spreadsheet is different from similar software used for business operations such as for accounting.
- **Risk-Based Analysis:** In this case, the software is only used to collect and display data for monitoring nonconformances, and the manufacturer has established additional process controls and inspections to ensure that nonconforming product is not released. Therefore, failure of the spreadsheet to perform as intended should not result in a quality problem that foreseeably leads to compromised safety. As such, the software does not pose a high process risk, and the assurance activities should be commensurate with the process risk.
- **Tested:** Spreadsheet X, Version 1.2
- **Test type:** Unscripted testing – exploratory testing

- **Goal:** Ensure that analyses can be correctly created, read, updated, and deleted
- **Testing objectives and activities:**
  - Create new analysis: Passed
  - Read data from the required source: Passed
  - Update data in the analysis: Failed due to input error, then passed re-test
  - Delete data: Passed
  - Verify through observation that all calculated fields correctly update with changes: Passed with noted deviation
- **Deviation:** During the testing of the update, when the user inadvertently input text into an updatable field requiring numeric data, the associated row showed an immediate error.
- **Conclusion:** The spreadsheet is acceptable for its intended use. Incorrectly inputting text into the field is immediately visible and does not impact the intended use. A new validation rule was placed on the field to permit only numeric data inputs. The testing was performed again with the validation rule and the update passed all testing objectives. No additional errors were observed in the spreadsheet functions after the validation rule was implemented.
- **When/Who:** July 9, 2025, by Jane Smith

B. Considerations for Electronic Records Requirements

Manufacturers have expressed confusion and concern regarding the application of 21 CFR Part 11, Electronic Records; Electronic Signatures, to computers or automated data processing systems used as part of production or the quality management system. Manufacturers should refer to the "Part 11, Electronic Records; Electronic Signatures – Scope and Application" guidance (hereafter referred to as the "Electronic Records guidance"), when determining whether and how to apply 21 CFR Part 11 (hereafter referred to as "Part 11").

The regulations in Part 11 set forth the criteria under which FDA considers electronic records, electronic signatures, and handwritten signatures executed to electronic records to be trustworthy, reliable, and generally equivalent to paper records and handwritten signatures executed on paper (see 21 CFR 11.1(a)). In general, Part 11 applies to records in electronic form that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in Agency regulations (see 21 CFR 11.1(b)). Part 11 also applies to electronic records submitted to the Agency under requirements of the FD&C Act and the Public Health Service Act (PHS Act), even if such records are not specifically identified in Agency regulations (see 21 CFR 11.1(b)). The underlying requirements set forth in the FD&C Act, PHS Act, and FDA regulations (other than Part 11) are referred to as "predicate rules." In addition, where electronic signatures and their associated electronic records meet the requirements of Part 11, FDA will generally consider the electronic signatures to be equivalent to full handwritten signatures, initials, and other general signings as required by agency regulations (21 CFR 11.1(c)).

For computer software used as part of production or the quality management system, the applicable predicate rules include those under Part 820. A document required under Part 820—including, but not necessarily limited to, a document Part 820 requires to bear a signature—and maintained in electronic form would generally be an "electronic record" under Part 11 (see

21 CFR 11.3(b)(6)). To determine when a record is required under Part 820, manufacturers should consider, among other things, whether the record would be necessary as evidence to document required validation. If a manufacturer maintains in electronic form a document required under Part 820, then Part 11 generally applies.

Example: Documentation demonstrating that a management enterprise system correctly and reliably automates checking materials before use in production would generally be necessary as evidence for a manufacturer to support a validated state. In this example, Part 11 would generally apply to the documentation if in electronic form.

Example: Upon application startup, a COTS automatically saves routine activity logs. However, in this case, these activity logs are not necessary as evidence for a manufacturer to support a validated state. In this example, Part 11 would not apply to the activity logs.

As discussed in the Electronic Records guidance, FDA intends to exercise enforcement discretion regarding specific Part 11 requirements for validation of computerized systems used to create, modify, maintain, or transmit electronic records (see 21 CFR 11.10(a) and 11.30). But the enforcement discretion policy described in the Electronic Records guidance (concerning validation of computerized systems used to create, modify, maintain, or transmit electronic records) expressly does not apply to validation requirements for computer software used as part of production or the quality management system arising under Subclauses 4.1.6, 7.5.6, and 7.6 of ISO 13485.

This guidance recommends that manufacturers base their approach to computer software assurance on a justified and documented risk assessment and a determination of the potential of the system to affect product quality, patient safety, and record integrity. Manufacturers may utilize a least-burdensome, risk-based approach outlined in this guidance to provide assurance that the software that maintains electronic records subject to Part 11 performs as intended.

Appendix A. Examples

The examples in this section outline possible application of the principles in this guidance to various software assurance situations.

Example 1: Nonconformance Management System

A manufacturer has purchased and configured COTS software for automating their nonconformance process and is applying a risk-based approach for computer software assurance in its implementation. The software is intended to manage the nonconformance process electronically.

As part of the assurance activities, the manufacturer performs a thorough assessment of the software vendor that includes:

- Evaluation of the vendor's software development life cycle,
- Review of the vendor's quality management system and relevant certifications, and
- Review of vendor's cybersecurity documentation and life cycle management plans as well as relevant certifications.

Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software's intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures.

The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:

GRZAN

Table 2. Computer Software Assurance Example for a Nonconformance Management System

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Nonconformance Initiation Operations: • A nonconforming event results in the creation of a nonconformance record. • The necessary data for initiation are recorded prior to completion of a nonconformance initiation task. • A Nonconformance Owner is assigned prior to completion of the nonconformance initiation task.	The intended uses of the operations are to manage the workflow of the nonconformance and to error-proof the workflow to facilitate the work and a complete quality record. These operations are intended to supplement processes established by the manufacturer for containment of non-conforming product.	Failure of the nonconformance initiation operation to perform as intended may delay the initiation workflow, but would not result in a quality problem that foreseeably compromises safety, as the manufacturer has additional processes in place for containment of non-conforming product, which include separation of affected product, alerting line management, and labeling the affected product. As such, the manufacturer determined the nonconformance initiation operations did not pose a high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. In addition, the manufacturer supplements these activities with exploratory testing of the operations. High level objectives for testing are established to meet the intended use and no unanticipated failures occur.	The manufacturer documents: • the intended use • result of risk-based analysis • summary description of the operations tested • the testing objectives and if they passed or failed • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
<u>Electronic Signature Function:</u> • The electronic signature execution record is stored as part of the audit trail. • The electronic signature employs two distinct identification components of a login and password. • When an electronic signature is executed, the following information is part of the execution record: o The name of the person who signs the record. o The date (DD-MM-YYYY) and time (hh:mm) the signature was executed. o The role of the signatory associated with the signature (such as review, approval, responsibility, or authorship).	The intended use of the electronic signature function is to capture and store an electronic signature where a signature is required and such that it meets requirements for electronic signatures.	Failure of the electronic signature function to perform as intended may compromise or delay compliance with regulatory requirements and established SOPs but would not result in a quality problem that foreseeably compromises safety. As such the manufacturer determined that the electronic signature function did not pose a high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. To provide assurance that the function complies with applicable requirements, the manufacturer performs scenario testing of this function with users to demonstrate the function meets the intended use.	The manufacturer documents: • the intended use • result of risk-based analysis • testing performed • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
<u>Product Containment Function:</u> • When a nonconformance is initiated for product outside of the manufacturer's control, then the system prompts the user to identify if a product correction or removal is needed.	This function is intended to trigger the necessary evaluation and decision-making on whether a product correction or removal is needed when the nonconformance occurred in product that has been distributed.	Failure of the function to perform as intended would result in a necessary correction or removal not being initiated, resulting in a quality problem that foreseeably compromises safety. The manufacturer therefore determined that this function poses high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. The manufacturer determined the function is a high process risk. The manufacturer performed assurance activities commensurate with the medical device risk and established a detailed scripted test protocol to exercise the possible interactions and potential function failures. The testing also included appropriate repeatability testing in various scenarios to provide assurance that the function works reliably.	The manufacturer documents: • the intended use • result of risk-based analysis • a detailed test protocol • detailed report of the testing performed • pass/fail results for each test case • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed • the signature and date of the signatory authority according to the manufacturer's established SOP

Example 2: Learning Management System (LMS)

A manufacturer is implementing a COTS LMS and is applying a risk-based approach for computer software assurance in its implementation. The software is intended to manage, record, track, and report on training.

As part of the assurance activities, the manufacturer performs a thorough assessment of the software vendor that includes:

- Evaluation of the vendor's software development life cycle, and
- Review of the vendor's quality management system and relevant certifications.

Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures.

The following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:

GRZAN

Table 3. Computer Software Assurance Example for an LMS

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Access Control, User Management, and Notification Functions: • Create and manage user log-on features (e.g., username and password). • Assigns trainings to users per the curriculum assigned by management. • The system notifies users of training curriculum assignments, completion of trainings, and outstanding trainings. • The system notifies users' management of outstanding trainings.	These functions are intended to manage user access, user workflow, and user notifications regarding training.	Failure of these features, functions, or operations to perform as intended would impact the integrity of the quality record but would not foreseeably compromise safety. As such, the manufacturer determined that the features, functions, and operations do not pose high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. In addition, the manufacturer supplements these activities with unscripted testing, applying error-guessing to attempt to circumvent process flow and verify the access controls of the system.	The manufacturer documents: • the intended use • result of risk-based analysis • a summary description of the failure modes tested • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed

GRZAN

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Record-keeping and Reporting Functions: • The system captures evidence of users' training completion. • The system generates reports on training curriculum assignments, completion of training, and outstanding trainings.	These functions are intended to capture and maintain evidence and records of user training completion and generate analytic reports on the records for review by the organization as needed.	Failure of these features, functions, or operations to perform as intended would impact the integrity of the quality record but would not foreseeably compromise safety. As such, the manufacturer determined that the features, functions, and operations do not pose high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and installation activities. In addition, the manufacturer supplements these activities with unscripted testing to "break" the system (e.g., try to delete the audit trail), verify record integrity, and the report generating functions.	The manufacturer documents: • the intended use • result of risk-based analysis • a summary description of the failure modes tested • any issues found • conclusion declaring acceptability including resolution of issues • record of who performed testing and date the testing was performed

GRZAN

Example 3: Business Intelligence Applications

A medical device manufacturer has decided to implement a commercial business intelligence solution for data mining, analytics, and reporting. The software is intended to better understand product and process performance over time, to identify improvement opportunities.

As part of the assurance activities, the manufacturer performs a thorough assessment of the software vendor that includes:

- Evaluation of the vendor's software development life cycle,
- Review of the vendor's quality management system and relevant certifications, and
- Review of vendor's cybersecurity documentation and life cycle management plans as well as relevant certifications.

Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures.

In addition to the vendor assessment, the following features, functions, or operations were considered by the manufacturer in developing a risk-based assurance strategy:

GRZAN

Table 4. Computer Software Assurance Example for a Business Intelligence Application

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Connectivity Functions: • The software allows for connecting to various databases in the organization and external data sources. • The software maintains the integrity of the data from the original sources and is able to determine if there is an issue with the integrity of the data, corruption, or problems in data transfer.	These functions are intended to ensure a secure and robust capability for the system to connect to the appropriate data sources, ensure integrity of the data, prevent data corruption, modify, and store the data appropriately.	Failure of these functions to perform as intended would result in inaccurate or inconsistent trending or analysis. This would result in failure to identify potential quality trends, issues or opportunities for improvement, which in some cases, may result in a quality problem that foreseeably compromises safety. As such, the manufacturer determined that these functions posed high process risk, necessitating more-rigorous assurance activities, commensurate with the related medical device risk.	The manufacturer determined assurance activities commensurate with the medical device risk and has performed an assessment of the system capability, supplier evaluation, and installation activities. Additionally, the manufacturer establishes a detailed scripted test protocol that exercises the possible interactions and potential ways the functions could fail. The testing also includes appropriate repeatability testing in various scenarios to provide assurance that the functions work reliably.	The manufacturer documents: • the intended use • result of risk-based analysis • detailed test protocol • a detailed report of the testing performed • pass/fail results for each test case • any issues found • conclusion declaring acceptability including resolution of issues found • record of who performed testing and date the testing was performed • the signature and date of the signatory authority according to the manufacturers established SOP

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
User help Feature: • The software provides the user a help menu for the application.	This feature is intended to facilitate the interaction of the user with the system and provide assistance on use of all the system features.	Failure of the feature to perform as intended is unlikely to result in a quality problem that would lead to compromised safety. Therefore, the manufacturer determined that the feature does not pose high process risk.	The feature does not necessitate any additional assurance effort beyond what the manufacturer has already performed in assessing the system capability, supplier evaluation, and installation activities.	The manufacturer documents: • the intended use • result of risk-based analysis • record of who performed the assessment and date the assessment was performed • conclusion declaring acceptability including resolution of issues

GRZAN

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Reporting Functions: • The software is able to create and perform queries and join data from various sources to perform data mining. • The software allows for various statistical analysis and data summarization. • The software can create graphs from the data. • The software provides the capability to generate reports of the analysis.	These functions are intended to allow the user to query the data sources, join data from various sources, perform analysis, and generate visuals and summaries. These functions are intended for collection and recording data for monitoring and review purposes that do not have a direct impact on production or process performance. In this example, the software is not intended to inform quality decisions.	Failure of these functions to perform as intended may result in a quality problem (e.g., incomplete or inadequate reports) but, in this example, would not foreseeably lead to compromised safety because these functions are intended for collection and recording data for monitoring and review purposes that do not have a direct impact on production or process performance. Therefore, the manufacturer determined that these functions do not pose high process risk.	The supplier of the reporting software has validated the ability of the software to create and perform queries, join data from various sources to perform data mining, perform statistical analysis and data summarization, create graphs and generate reports. Beyond this, the manufacturer has assessed the system capability and performed supplier evaluation and installation activities. As such, the manufacturer determined that the reporting functions of the software do not necessitate any additional assurance effort beyond these activities.	The manufacturer documents: • the intended use • risk-based analysis • record of who performed the assessment and date the assessment was performed • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues

GRZAN

Example 4: Software as a Service (SaaS) Product Life Cycle Management System (PLM)

A medical device manufacturer has decided to implement a SaaS-based Product Life Cycle Management System (PLM). While the PLM SaaS solution has the capability to automate the management of various life cycle stages of a product development, the manufacturer intends to use the solution for broad project management. The SaaS PLM is intended to automate the intake of project requirements, develop project plans, monitor/track project execution, and maintain relevant records, signatures, and deliverables upon project closing. This intended use of the system does not directly impact patient safety or product quality but does maintain a quality record where integrity of the data is needed. The manufacturer does not need any customization of the "out-of-the-box" capabilities of the SaaS product and only needs to perform basic standard configuration of the SaaS product (e.g., user roles, accounts).

As part of the assurance activities, the manufacturer performs a thorough assessment of the SaaS vendor that includes:

- Evaluation of the vendor's software development life cycle,
- Review of the vendor's quality management system and relevant certifications,
- Review of vendor's cybersecurity documentation and life cycle management plans as well as relevant certifications, and
- Review of the vendor's infrastructure support including availability and reliability.

Based on the manufacturer's established SOP for evaluating suppliers, the vendor's capability to meet the manufacturer's requirements are deemed acceptable for the software intended use. The manufacturer maintains a record of the evaluation according to their established purchasing control procedures. The manufacturer also establishes a service agreement with the SaaS vendor that includes requirements for security, data integrity, privacy, availability, change management, and business continuity.

Automatic Updates:
The SaaS vendor provides the manufacturer documentation summarizing the changes, testing, and testing results of all automatic updates made to the SaaS system functions identified by the manufacturer as part of the service agreement. The manufacturer performs an assessment of the changes and the effect they may have on the intended use. The manufacturer performs risk-based assurance testing of the changes appropriate to the impact identified. The manufacturer maintains a record summarizing the risk assessment of the change and any assurance activities performed.

GRZAN

Table 5. Computer Software Assurance Example for SaaS PLM

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Project Initiation and Planning Function: • The software allows for the creation of a new project. • The software is able to assign team members and roles to the project as assigned by the manufacturer's management. • The software intakes and updates project requirements and specifications. • The software is able to develop a project plan, with tasks, dependencies, milestones, and deliverables. • The software monitors changes to data maintained by the project record.	These functions are intended to automate the creation of a data record for the project, maintain user roles, assign responsibilities for key project data to team members, intake the key data relevant to the project, maintain the integrity and associations of the project data, and monitor changes or updates to the project information.	Failure of these functions to perform as intended would impact the integrity of the quality record, but would not foreseeably compromise safety. As such, the manufacturer determined that the functions do not pose high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and established service agreements with the SaaS vendor. Based on the risk-based analysis, the manufacturer performs a configuration verification and User Acceptance Testing (UAT) using exploratory unscripted testing.	The manufacturer documents: • the intended use • risk-based analysis • summary description of the objectives tested, and testing performed • any issues found • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues • record of who performed assessment and date the assessment was performed

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
Electronic Signature Function: • The electronic signature execution record is stored as part of the audit trail. • The electronic signature employs two distinct identification components of a login and password. • When an electronic signature is executed, the following information is part of the execution record: o The name of the person who signs the record. o The date (DD-MM-YYYY) and time (hh:mm) the signature was executed. o The meaning associated with the signature (such as review, approval, responsibility, or authorship).	The intended use of the electronic signature function is to capture and store an electronic signature where a signature is required and such that it meets requirements for electronic signatures.	Failure of the electronic signature function to perform as intended may compromise or delay compliance with regulatory requirements and established SOPs but would not result in a quality problem that foreseeably compromises safety. As such the manufacturer determined that the electronic signature function does not pose a high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and configuration activities. To provide assurance that the function complies with applicable requirements, the manufacturer performs scenario testing of this function with users to demonstrate the function meets the intended use.	The manufacturer documents: • the intended use • risk-based analysis • testing performed • any issues found • record of who performed testing and date the testing was performed • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues

GRZAN

Features, Functions, or Operations	Intended Use of the Features, Functions or Operations	Risk-Based Analysis	Assurance Activities	Establishing the appropriate record
<u>Access Control and Traceability Functions:</u> • The function controls user roles, associated permissions, and system access (e.g., user log-on). • The function monitors and maintains records of access and modifications of the final data records maintained in the system. • The function produces time stamped reports of the system access, authorization, change, and the associated user for modifications made to final data records maintained in the system as established by the manufacturer's procedure for auditing.	These functions are intended to provide appropriate access control, establish user roles, and maintain individual user accounts. The functions are also intended to monitor, maintain, and report a time-stamped logging of access or changes to the training records or electronic signature events to ensure the authenticity, reliability, and integrity of the final records established by the manufacturer to be maintained.	Failure of these functions to perform as intended has a significant impact on the overall intended use and system operations, and as such, may result in a quality management system integrity and compliance issue. Since these functions are intended to ensure integrity of the data record for a quality management system requirement only, the manufacturer determines that a failure to perform as intended would not foreseeably lead to compromised safety and therefore does not pose a high process risk.	The manufacturer has performed an assessment of the system capability, supplier evaluation, and established service agreements with the SaaS vendor. Based on the risk-based analysis, the manufacturer performs a configuration verification and develops an automated test script that will quickly exercise the access controls to also support verification of future changes. Additionally, the manufacturer performs User Acceptance Testing (UAT) of the reporting capabilities using exploratory unscripted testing.	The manufacturer documents: • the intended use • risk-based analysis • summary of automated test cases in the test script (or electronic version of the test script) and a summary description of the objectives tested, and testing performed • any issues found and results of the automated test script • conclusion declaring acceptability including resolution, justification, and/or process controls implemented addressing the impact of the issues • record of who performed testing and date the testing was performed

Guidance History[*]	Date	Description
Revisions to Final Guidance	February 2026	Revisions issued under Level 2 guidance procedures (21 CFR 10.115(g)(4)), including revisions to align with the amendments to 21 CFR 820 (the Quality Management System Regulation (QMSR)). This guidance supersedes the final guidance titled "Computer Software Assurance for Production and Quality System Software," issued September 2025.
Level 1 Final Guidance	September 2025	See Notice of Availability for the guidance "Computer Software Assurance for Production and Quality System Software" for more information.**

*This table was implemented, beginning September 2025, and previous guidance history may not be captured in totality.
**The Notice of Availability is accessible via the Search for FDA Guidance Documents webpage.