Computer Software Assurance for Production and Quality System Software - Draft Guidance
October 27, 2022

Moderator: CDR Kim Piermatteo

CDR Kim Piermatteo: Hello and welcome to today's CDRH webinar. Thank you for joining us today. This is Commander Kim Piermatteo of the United States Public Health Service, and I serve as the Education Program Administrator in the Division of Industry and Consumer Education in CDRH's Office of Communication and Education, and I'll be your moderator for today's program.

Our topic today is the draft guidance titled Computer Software Assurance for Production and Quality System Software. The FDA believes that applying a risk-based approach to computer software used as part of medical device production or the quality system would better focus manufacturers' assurance activities to help ensure product quality while helping to fulfill the validation requirements within Title 21 of the Code of Federal Regulations, or CFR, Part 820.70(i).

We're holding this webinar to provide you with an opportunity to learn more and to answer any questions you may have about this draft guidance.

It's my pleasure now to introduce you to our presenter for today's program, Francisco Vicenty, Case for Quality Program Manager on the Compliance and Quality Staff within CDRH's Office of Product Evaluation and Quality, or OPEQ. We'll begin with a presentation from Cisco and then field your questions about this topic.

As a friendly reminder, for those of you participating live in today's CDRH webinar, please be sure you have joined us via the Zoom app and not through a web browser to avoid any technical issues. Thank you all again for joining us. I'd now like to turn it over to Cisco to start today's presentation. Cisco.

Cisco Vicenty: Thank you, Kim. Hello, my name is Cisco Vicenty, and I am the Program Manager for the Case for Quality within the Office of Product Evaluation and Quality in CDRH.

The webinar today focuses on the draft guidance released on September 13, 2022, regarding Computer Software Assurance for Production and Quality System Software.

The objectives for this webinar are to provide you with the information necessary to identify and describe the scope and purpose of the draft guidance, describe Computer Software Assurance, CSA, as a risk-based approach to establish confidence in automation used for medical device production or quality systems, and describe some of the risk-based assurance activities that may be applied to established CSA.

Advances in manufacturing technologies, including the adoption of automation, robotic simulation, and other digital capabilities, enable manufacturers to reduce source 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 of these technologies.

FDA has engaged with stakeholders via the Medical Device Innovation Consortium, MDIC, site visits the medical device manufacturers, and through benchmarking efforts with other industries, such as automotive and consumer electronics, to really keep abreast of the latest technologies and better understand our stakeholders' challenges and any opportunities for further advancement.

Medical device manufacturers have expressed 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 system. Given the rapidly changing nature of software, manufacturers have also expressed desire for more iterative, agile approach for validation of these computer softwares.

With that background, now, onto the guidance.

In order to facilitate and foster the adoption and use of innovative technologies that promote patient access to high-quality medical devices, this draft guidance provides recommendations on computer software assurance for computers and automated data processing systems used as part of medical device production or the quality system. It also describes CSA as a risk-based approach to establish confidence in that automation used for production or quality systems. The guidance also describes various methods and testing activities that may be applied to establish that software assurance and provide objective evidence to fulfill any regulatory requirements. When final, this guidance will supersede section 6 validation of automated process equipment and quality system software of the general principles of software validation guidance that was published in January 2002.

This draft guidance provides recommendations applicable to the requirements of 21 CFR 820.70(i), automated processes. This requirement states, when computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software for its intended use according to an established protocol. All software changes shall be validated before approval and issuance, and finally, each validation activities shall be documented. So when we talk about what's in scope of that regulatory requirement, this includes, but it is not limited to software for design, development, manufacturing, or the quality system. What is not in scope of what this guidance covers is software that is used as a medical device, or SaMD space, or software in a medical device, or SiMD space.

Now, onto CSA.

So what is CSA? Computer software assurance is a risk-based approach for establishing and maintaining confidence that software is fit for its intended use. The approach considers a risk of compromised safety and the quality of the device should the software fail to perform as intended, to determine the level of assurance effort and activity is appropriate to establish confidence in the software. Manufacturers increasingly rely on computers and automated processing systems to monitor and operate production, alert responsible personnel, transfer and analyze production data, among other uses.

In addition, manufacturers establish and maintain that the software used in production or the quality system is in a state of control throughout its lifecycle. This is the validated state. By applying principles such as a risk-based testing, unscripted testing, continuous performance monitoring, and data monitoring, as well as validation activities that are performed by other entities, such as developers, suppliers, vendors, the computer software assurance approach provides flexibility and agility in helping to assure that the software maintains a validated state consistent with 21 CFR 820.70(i). Because the computer software assurance is risk-based, the burden of validation is no more than necessary to

address the identified risk. This approach supports efficient use of resources, in turn, promoting more product quality.

This guidance outlines an approach that is intended to help manufacturers establish a risk-based framework for computer software assurance throughout the software's lifecycle. The approach outlines a sequential flow for consideration. First, identify the intended use of software used as part of production/quality system.

Second, evaluate the level of risk if the software were to fail to perform as intended. Three, determine the assurance activities to perform commensurate with that risk. And finally, establish the appropriate record with sufficient evidence to demonstrate that the software was assessed and performs as intended. So we're going to cover these steps in more detail in the following slides.

21 CFR 820.70(i) requires manufacturers to validate software that is used as part of production or the quality system for its intended use. The guidance recommends manufacturers first determine if the requirement applies. To determine this, it is recommended many factors consider, will the software be used directly as part of production and the quality system?

For example, is our software intended for automating production processes, inspection, testing, or the collection and processing of production data? Software intended for automated quality system processes, collection, and processing quality system data or maintaining quality record established under quality system regulation. Alternatively, the software may be used to support production of the quality system.

And for example, this could be software that's 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 system. For example, such as those used for developing and running scripts or software intended for automating general recordkeeping that is not part of the quality record. Both kinds of software are used as part of production supply system and must be validated under 21 CFR 820.70(i).

However, the supporting software often carries lower risk. On their risk-based computer software assurance approach, the effort of validation may be reduced accordingly without compromising safety. If the software will not be used directly to support production or the quality system, for example, these are software intended for management general business processes or operations such as email, accounting application, software that is intended for establishing or supporting infrastructure not specific to production or the quality system, such as networking, content of operations, then the requirements of 21 CFR 820.70(i) would not apply. It is a good practice for a company to make sure the system works for their intended use, but this is not in scope of the regulatory requirements.

In the guidance, we recognize a software used as production or the quality system is often complex and comprised of several features, functions, and operations. Software may have more than-- may have one or more intended uses depending on the individual features, functions, and operations of the software. In cases where the individual features, functions, and operations have different roles within production of the quality system, they may present different risks with different levels of validation effort. FDA recommends that manufacturers examine the intended use of those 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.

Now, let's discuss that risk-based approach. Once the intended use has been established, the level of risk if the software were to fail to perform as intended can be determined. This guidance discusses both process risks and medical device risks. A process risk refers to the potential to compromise production or the quality system. A medical device risk refers to the potential for a device to harm the patient or the user.

This guidance focuses on the medical device risk resulting from quality problems that compromises safety. A software feature function operation poses a high process risk when its failure to perform as intended may result in a quality problem that foreseeably compromises safety, meaning an increased medical device risk. This process of risk identification step focuses only on the process as opposed to the medical device risk posed to the patient or user.

Examples of software intended uses that are generally high process risks are those that maintain process parameters. We're talking about temperature, pressure, humidity, that affect the physical properties of the product or manufacturing processes that are identified as essential to device safety or quality. Measure, inspecting, analyzing, or determining acceptability of product or process with limited or no additional human awareness or review, performing process corrections or adjustments of process parameters based on data monitoring or automatic feedback from other process steps without additional human awareness or review, or producing directions for use or other labeling provided to patients and uses that are necessary for safe operation of the medical device.

Additionally, it could be used automating surveillance trending or tracking data that the manufacturer identifies as essential to device safety and quality. Software feature function operation does not 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 a situation 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 these intended uses are those that collect and report data from the process for monitoring and review purposes that do not have a direct impact on production process performance, uses that aren't part of the quality system for corrective or preventive action routing, automated logging, tracking of complaints, automated change control management, or automated procedure management. Uses are intended to manage data, processed or unorganized data, automate an existing calculation, increase process monitoring and provide alerts when an exception occurs in the established process, and/or uses that are intended to support production of the quality system. FDA acknowledges that process risks associated with software uses as part of production acquired system are on a spectrum ranging from high risk to low risk. Manufacturers determine the risk of each software feature, function, 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. Therefore, for the purpose of this guidance, FDA is presenting the process risks in a binary manner, high process risk, not high process risk. A manufacturer may still determine that process risk is, for example, moderate, intermediate, or even low for the purposes of determining assurance activities. In such a case, the portion of this guidance concerning not high process risk would apply.

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 and effort. After determining the risk, when deciding on the appropriate assurance activities, FDA also recommends manufacturers consider whether there are any additional controls or mechanisms in place throughout the quality system that may decrease the impact, compromise safety and/or quality if failure of a 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, the activities, people, and established processes that provide control in production.

Such activities may include procedures to ensure integrity in the data supporting production, or software quality assurance processes performed by other organizational units, establish purchasing control processes for selecting and monitoring software developers, for example, the manufacturer could incorporate the practices, validation work, and electronic information already performed by developers of software as a 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 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 are periodically continuously collected by the software for the purposes of monitoring or detecting issues and anomalies in the software after implementation of that software. The capability to monitor and detect performance issues or deviations in system errors may reduce the risk associated with a failure of the software to perform as intended. And this may be considered when deciding on the assurance activities.

The use of computer system validation tools, such as a bug tracker, automatic testing for the assurance of software used in production as part of the quality system whenever possible, the use of testing done in iterative cycles and continuously throughout the life cycle of software used in production as part of the quality system. All of these activities that typically go on within a manufacturer can be part of building out a comprehensive assurance approach. In cases where the quality problem may foreseeably compromise safety, those high process risk cases, the level of assurance should be commensurate with the medical device risk.

A feature, function, or operation that could lead to severe harm to a patient or user would generally be a high device risk. In contrast, a feature, function, or operation that would not foreseeably lead to severe harm would likely not be a high 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. These may include a greater amount of objective evidence. Conversely, relatively less risk and not a high process risk of compromise safety and equality generally entails less collection of objective evidence for the computer software assurance effort.

Additionally, FDA recommends manufacturers include current practices around testing as part of the assurance activities they may leverage. These include unscripted testing, dynamic testing in which the tester's actions are not prescribed by written instructions. In a test case, this includes ad hoc testing, error guessing, exploratory testing, or scripted testing, the dynamic testing in which the tester's actions are prescribed by written instructions in a test case. Scripted testing could come in the variety of a robust scripted test or a limited scripted test. What isn't clearly important to know is that unscripted testing does not mean undocumented. And we'll cover that in the next slide.

Finally, the draft guidance provides recommendations on establishing the appropriate record of the activities performed. When establishing the record, the manufacturers should capture sufficient objective evidence to demonstrate that the software feature, function, or operation was assessed and performs as intended. The record should include the following, the intended use of software feature, function, or operation, the termination of risk of the software feature, function, or operation, documentation of the assurance activities conducted, including description of the testing conducted based on the assurance activity, issues found, any deviations, failures, and how they were dispositioned, conclusion statement declaring acceptability of the results, the date of testing or assessment and the name of the person who conducted the testing and assessment, and, when established, the review and approval, when appropriate, when necessary, a signature and date of an individual with control authority, and that is dependent on how you've established your processes and procedures.

Documentation of assurance activities need not include more evidence than necessary to show the software feature, function, or operation performs as intended for the risk identified. FDA recommends the record retain sufficient detail of the activity to serve as a baseline for improvement or as a reference point if issues occur. Additionally, we recommend manufacturers review section D of the guidance for more examples of what to include in the record of activities.

Advances in digital technology may allow manufacturers to leverage automated traceability testing and electronic capture of work performed to document the results, reducing the need for manual or paper-based documentation. As the least burdensome method, FDA recommends the use of electronic records, such as system logs, audit trails, and other data generated by software as opposed to paper documentation and screenshots in establishing the record associated with the assurance activities.

Let's quickly talk about the electronic record requirements.

Inevitably, when we discuss records in electronic format, part 11 comes into focus. In general, part 11 applies to records in electronic format that are created, modified, maintained, archived, retrieved, or transmitted under any records requirements set forth in agency regulations. Part 11 also applies to electronic records submitted to the agency under requirements of the Federal Food, Drug, and Cosmetic Act, and 594 of the Public Health Service Act, even if such records are not specifically identified in the agency regulations.

As described in part 11, Electronic Records Electronic Signature Scope and Application Guidance, the agency intends to exercise enforcement discretion regarding part 11 requirements for validation of computerized systems used to create, modify, maintain, or transmit electronic records. Despite existing guidance, manufacturers have expressed confusion and concern regarding the application of part 11, electronic records, electronic signatures to computers or automated data processing systems used as part of production or the quality system. We want to highlight that as part of the comment period for

this guidance, we also invite comments or questions regarding the application of 21 CFR Part 11 requirements to systems in scope of 21 CFR 820.70(i).

Let's discuss providing comments on the draft guidance.

You may comment on any guidance at any time. So let's just lay that out there right from the very beginning. But in this particular case, if you're going to submit comments on the draft guidance prior to the closure date, which is November 14, 2022, it helps ensure that FDA considers your comments on the draft guidance before we start work on the final guidance.

On this slide, you'll find the link to the docket and where you can provide comments to the guidance and a link to the draft guidance. Once again, just providing a reminder that the comments to the dockets should be submitted by November 14. We've also provided links to useful guidances and references that were used throughout the presentation for you to be able to quickly access as needed.

As we close out the presentation, please remember, computer software assurance is a risk-based approach to establish confidence in the automation used for production or quality systems. The approach features four steps-- identifying that intended use, determining the risk-based approach that will be utilized, determine the appropriate assurance activities, and finally, establishing the appropriate record. Once again, we invite you to provide comments and ask questions about this draft guidance.

With that, I want to thank everybody for their time. And now, we'll move on to questions and answers.

CDR Kim Piermatteo: Thank you, Cisco, for that presentation. At this time, I'd now like to introduce our additional panelists who will be joining Cisco for the live question and answer segment of today's program.

First, we have Ian Ostermiller, Policy Advisor in CDRH's Office of Policy, and Mary Wen, Regulatory Policy Analyst within CDRH's Office of Product Evaluation and Quality, or OPEQ.

Before we begin taking your live questions, I'd like to go over a few reminders. Foremost, to ask a question, please select the Raise Hand icon, which should appear on the bottom of your Zoom screen. I'll announce your name and give you permission to talk. When prompted, please select the blue button to unmute your line and then ask your question. After you ask your question, please lower your hand. If you have another question, please raise your hand again to get back into the queue, and I will call on you as time permits. And lastly, please remember to limit yourself to one question only, and try to keep it as short as possible.

Now, as we wait to receive some of your questions, I'd like to welcome our additional panelists with a few questions that we've gotten since the draft guidance was issued.

For our first previously received question, I'll be directing that to you Ian. Ian, the question is, how does FDA'S guidance on electronic records apply to the approach this draft guidance lays out for software validation requirements?

Ian Ostermiller: Hi, Kim. Thanks for the introduction. I'm Ian Ostermiller. Again, I'm a Policy Advisor in CDRH's Office of Policy.

And how this draft guidance relates to the electronic records requirements under Part 11 is this draft guidance focuses on a risk-based approach for fulfilling the requirements in 21 CFR 820.70(i), that's specifically for validation of software used in computers and automated data processing systems that are used as part of medical device production or the quality system. Part 11 has a separate validation requirement for electronic records. And in the Part 11 guidance, Part 11 Electronic Records, Electronic Signatures, Scope and Application, we state the FDA is exercising enforcement discretion with respect to that validation requirement. However, again, that is separate from the validation requirement that this draft guidance discusses.

The Part 11 guidance also talks about what FDA considers to be electronic records for purposes of Part 11. And it introduces the concept of predicate rules. Under the Part 11 guidance 820.70(i) would be a predicate rule.

Nonetheless, we understand that manufacturers may still have questions about how to apply Part 11 in relation to satisfying the requirements of 21 CFR 820.70(i) as well as how to satisfy the other requirements within Part 11 for electronic records created in validating computer software used in data processing or quality systems. To help us provide better guidance in the final draft, we are interested in better understanding your specific questions or concerns, and we encourage manufacturers to submit comments to the docket for FDA to consider.

CDR Kim Piermatteo: Thank you, Ian. Alright, now for our next previously received question. I'll be directing that to you, Mary. Mary, the question is, how will investigators be trained on the CSA guidance?

Mary Wen: Thanks, Kim, and thanks for the introduction. Again, I'm Mary Wen, I'm a Regulatory Policy Analyst in the Office of Product Evaluation and Quality. And the answer to that is that when the guidance is finalized, we intend to work with our investigators to ensure awareness and appropriate training on the principles outlined in the guidance. Thank you.

CDR Kim Piermatteo: Thanks, Mary. Alright, we are going to go ahead and take our first live question. John, I have unmuted your line. Please unmute yourself and ask your question.

John Ruckstuhl: Sure. This is John. And can you tell me, is it fair to say that the terms IQ, OQ, PQ, these are terms that are really no longer in currency with regard to this topic? Am I right? That's it.

CDR Kim Piermatteo: Thank you, John, for that question. Cisco, would you like to provide a response?

Cisco Vicenty: Absolutely. So one of the things to consider with regards to the terms IQ, OQ, PQ-- and this actually falls all the way back to the original general principle of software validation guidance. I think the discussion at that point in time was that IQ, OQ, PQ, while it is relevant from a process standpoint, a process-validation piece, doesn't necessarily apply when you're talking about the software validations cases. So it isn't a situation where it's not relevant or applicable. We've always left it up to the manufacturers to build the process to accommodate whatever was needed for their quality system or for their own business objectives. If utilizing those terms puts things into context for the organization, they're free to open them. But it isn't something that we've stated beforehand is really applicable or necessary from the software validation state.

CDR Kim Piermatteo: Thank you, John, for that question. And thank you, Cisco, for that response. Our next question is coming from Shruthi Kumar? I apologize. I have unmuted your line. Please unmute yourself and ask your question.

Shruthi Kumar: Hello, panelists. My name is Shruthi Kumar. There is a discussion on the unscripted testing where you mention unscripted does not mean undocumented. I get that. But can we use the term abridged instead of unscripted where we are talking about minimalistic documentation versus a more scripted documentation and a scripted testing?

Cisco Vicenty: So I can respond to that piece. And I think it's fair to provide that feedback in the comments. The reason for using unscripted was really to just stay aligned with just current practices and other standards that exist out there around software testing.

Shruthi Kumar: OK, thank you. And I'm allowed to ask more questions, or should I again raise my hand?

CDR Kim Piermatteo: We would prefer you to raise your hand again and get back in the queue, and then I'll call on you if time permits.

Shruthi Kumar: OK, thank you.

CDR Kim Piermatteo: Thank you. Alright, our next question is coming from Parth. Parth, I have unmuted your line. Please unmute yourself and ask your question.

Parth: Hello. The guideline states that computer software assurance can be applied to a software that is being used to manufacture medical devices. But is it fair to say that the same guideline can be used to validate software across any GNB environment for manufacturing pharmaceuticals or other similar use cases?

CDR Kim Piermatteo: Thank you, Parth, for that question. I'm going to look to Cisco. Do you want to start by providing a response? Or Mary?

Mary Wen: This is Mary, and I'm happy to answer. So this guidance has been prepared by the Center for Devices and Radiological Health and the Center for Biologics Evaluation and Research in consultation with the Center for Drug Evaluation and Research, Office of Combination Products and Office of Regulatory Affairs. Specifically, this guidance provides-- or I should say this draft guidance provides-- recommendations regarding the requirements outlined in 21 CFR 820.70(i), which states that when computers or automated data processing systems are used as part of production or the quality system, the manufacturer shall validate computer software for its intended use according to an established protocol. All software changes shall be validated before approval and issuance.

These validation activities and results shall be documented. And when final, this draft guidance will supersede Section 6 of the General Principles of Software Validation Guidance. If you have any comments or questions regarding scope, we encourage you to submit comments to the docket so that they can be considered in finalization of this guidance. Thank you.

CDR Kim Piermatteo: Thanks, Mary.

Parth: Alright.

CDR Kim Piermatteo: Thanks, Parth. Alright, our next question is coming from Robin. Robin, I have unmuted your line. Please unmute yourself and ask your question.

Robin Gergen: Thank you. Can you hear me?

CDR Kim Piermatteo: Yes, we can. Just speak a little louder please.

Robin Gergen: OK, great. Sorry if I missed this. But do when the guidance is expected to be final?

CDR Kim Piermatteo: Thanks, Robin, for that question. I'm going to turn that one over to Mary. Mary, would you like to provide a response?

Mary Wen: Yes, I'm happy to, Kim. And so no, we do not know at this time when the guidance will be finalized. But we would want to make sure that we consider all the comments that we receive carefully in finalization of the guidance. Thank you.

Robin Gergen: Thank you.

CDR Kim Piermatteo: Thanks, Mary. Thanks, Robin. Don't forget about the docket. Submit comments to the docket. Alright, our next question is coming from Evgeni. Evgeni, I've unmuted your line. Please unmute yourself and ask your question.

Evgeni Nudelman: Hello. Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Evgeni Nudelman: Can you hear me?

CDR Kim Piermatteo: Yes, we can.

Evgeni Nudelman: Can anybody hear me?

CDR Kim Piermatteo: Evgeni, we can hear you. Can you not hear us?

Evgeni Nudelman: Can you hear me?

CDR Kim Piermatteo: We can hear you. I don't think you can hear us, so we're going to go ahead and move on to the next caller. Yogesh, I have unmuted your line. Please unmute yourself and ask your question.

Yogesh: Yeah, thanks, Kim. So CSA is emphasizing mainly on 21 CFR 820.70(i), right? And the reg-- the regulation says that validation is performed according to an established protocol, which means the regulation is saying, like, every testing, whatever we do, is done through established protocol. But now, with unscripted testing, I see that conflicts with that statement because unscripted testing also has ad hoc testing, which may not have any pre-approved established protocol. So are we planning to update the regulation as well if needed based on unscripted testing? Thank you.

CDR Kim Piermatteo: Thank you for that question. Cisco, would you like to provide a response?

Cisco Vicenty: Sure thing. So I think the piece of this that we've been trying to articulate is that there is a lot of flexibility in that understanding of what an established protocol is. And I think, as we've mentioned beforehand, even with the unscripted testing, there isn't a situation where we're saying do not document.

What we're talking about, even within that case, you are still laying out some objectives that need to be exercised, or accomplished, or get captured in some way, shape, or form. And within that context, there is a lot of flexibility with regards to developing what is a protocol established under the regulation. So there isn't, at least in this case-- and again, we're open to comments in the docket, and you need to revisit the regulation. It is just a situation of reassessing what we are looking for within the context of that protocol.

CDR Kim Piermatteo: Thank you, Cisco. Alright, our next question is coming from Saidhula, Saidhulu. I've unmuted your line. Please unmute yourself and ask your question.

Saidhulu Nalla: Yeah, good morning.

CDR Kim Piermatteo: Good morning.

Saidhulu Nalla: So my question is that our GMP regulatory environment, the regulation 21 CFR 211.68, it talks about the validation. Still this year [INAUDIBLE] will be applicable to that, or it is only applicable to medical devices?

CDR Kim Piermatteo: Thank you for that question. I think at this point-- Cisco, would you like to provide a response or seek additional clarification? Or Mary? I apologize. I'm sorry.

[INTERPOSING VOICES]

Cisco Vicenty: Go ahead, Mary.

Mary Wen: Go ahead, Cisco.

Cisco Vicenty: I could take a crack at it, and Mary can add. But I think, as Mary mentioned beforehand, this was targeting and addressing what were the outlined requirements of the 820.70(i) reg for medical devices and quality system activities. Now, the comments that you made here was the idea that this will supersede what is in the general principles of software validation guidance once this is final. Anything that uses that as a reference, this becomes part of that body of knowledge. I think with regards to what's going on in the 211 space, there's other guidances and other standards out there, I believe, that are our sister centers also referenced that outline principles just as this. Because a lot of these were built in conjunction with things that exist out there already.

Mary Wen: Thank you, Cisco. I don't have anything further. Thank you.

CDR Kim Piermatteo: Great. Thank you, Cisco, and thank you, Mary.

Saidhulu Nalla: Thank you.

CDR Kim Piermatteo: Alright, our next question is coming from Himanshu. Himanshu, I've unmuted your line. Please yourself and ask your question.

Himanshu Bedwal: Yep, hi. So good morning. So my question is, we talk about risk-based approach in the CSA. So is there any specific guideline what risk-based approach should be followed [INAUDIBLE] we have in the GAM5, like detectability, severity, and probability? So we are going to have that kind of details around risk-based approach, or it should be open ended?

Cisco Vicenty: So I think with regards to details, we in this case are leaving it open ended. But we are-- GAM5 has a well-established framework and has been a resource for a lot of the work done for a long time. There is nothing, I think, in here that is not aligned with that from any standpoint. But we weren't going to prescribe what the mechanism of establishing that risk is. I think the goal here is to really try to make sure that you're thinking through critically what is that intended use of the system and where the actual risk gets introduced.

Himanshu Bedwal: OK. Thank you.

CDR Kim Piermatteo: Thank you for that question. Alright, our next question is coming from Karoll. Karoll, I have unmuted your line. Please unmute yourself and ask your question.

Karoll Gonzalez: Thank you so much. My question is, what is the expectation for manufacturers in reference to the usage of requirements, functional specifications, and risk analysis based on the general principles of software validation? And it comes because the guidance mentions features, functions, and operations rather than requirements. What is the expectation in this case? Thank you.

Cisco Vicenty: Yeah, so I think the general principles of validation guidance and the focus on bringing in those requirements is still a general-- well, it's a well-established practice. The recommendations in that guidance are still valid, and we stand by that. The idea of introducing the focus on features, functions, and operations was just based on learnings and feedback that we've received where, given the complexity of some of the ways systems are evolving nowadays, not everything is applicable, nor does everything that is really not being utilized by the manufacturer need to be covered in the scope of a validation activity. And by parsing it down to a degree, it gives some flexibility to manufacturers to think through their validation strategy.

CDR Kim Piermatteo: Thanks, Cisco. Alright, our next question is coming from Maximilian. Maximilian, I've unmuted your line. Please unmute yourself and ask your question.

Maximilian Vogtland: Hey there. I have a question about the assurance activities. Is it possible to decide based on the intended use and based on the risk assessment that no further assurance activities are needed? Or is there a minimum of assurance activities we have to perform?

Cisco Vicenty: So there isn't a minimum of assurance activities outlined. The example there just is trying to make the point that, in that case, how it's being utilized given the risk, enough is done in just some of that assessment and evaluation piece to provide that level of confidence that the software will perform as it's intended and to really try to drive home the point that there isn't a lot of additional work that should be required as an organization to do that.

Again, always open to thoughts and comments put in dockets of better ways to articulate how that gets across. But as an organization, you should be thinking through, again, what are the risk pieces that are introduced with the software being implemented, and what is the actual work that needs to be done to assure that? In one case, it may just be this level of work as highlighted in the example. And in other cases, you may need to go a little further based on your intended use in your application.

CDR Kim Piermatteo: Thank you, Maximilian. And thank you, Cisco. Alright, our next question is coming from Pyroja. Pyroja, I've unmuted your line. Please unmute yourself and ask your question.

Pyroja Sulaiman: Hi, Kim. Thank you. So my question is whether this guidance applies to the regulatory document management systems like submission, document manage systems, et cetera.

Cisco Vicenty: In that sense, if you're looking at things that are housing and holding things from the quality system or quality record standpoint, the guidance here would be one that would apply in that case even those systems.

Pyroja Sulaiman: Thank you very much.

CDR Kim Piermatteo: Thank you. Alright, our next question is coming from Nellie. Nellie, I have unmuted your line. Please unmute yourself and ask your question.

Nellie Bushman: Hi. Good morning. Nellie Bushman. I work with a ton of small startups that use electronic data like DocuSign, or and they use SharePoint. Will those types of applications be able to use this standard, or are they going to be pushed to Part 11? Or is it-- can I use the risk-based approach is what I'd like to know on that.

Cisco Vicenty: So I think, as Ian mentioned beforehand, Part 11 outlines certain things from-- expectations and requirements from a record keeping standpoint. But they've put under enforcement discretion any additional validation requirements of Part 11. And I believe they also mentioned that the intent there is not to add any additional validation burden that isn't already covered by one of the predicate rules.

So I go back to the notion that if it is a system being utilized, in this case, that falls on the 820.70(i), you're applying whatever you need, and the guidance here will help, again, provide a set of recommendations. It isn't the only way to do things for that space. But within that, you've got to weigh and consider what are the extra requirements that might need to be looked at from a Part 11 standpoint.

Nellie Bushman: Now, what we've also noticed-- and this is just clarity-- is a lot of the systems are now providing whitepapers on how they comply where they've actually-- it looks like they've done their own validation. Could you pull that in and use the risk-based approach?

Cisco Vicenty: So I think, yeah, one of the things that we've outlined in the guidance is the ability-- and not even the ability, you should have been able to do beforehand-- but leveraging what those vendors provide as part of your assessment and determination on risk.

Nellie Bushman: Thank you very much.

Ian Ostermiller: Hi. This is Ian Ostermiller. And I just want to clarify that there are two separate validation requirements. And 820.70(i) deals only with those software systems involved in the quality system. It may be that other records outside of the quality system fall under the Part 11 guidance. And in that guidance, we suggest that your decision to validate computerized systems-- so something outside of what we're talking about with 820.70(i)-- should take into account the impact the systems have on your ability to meet the predicate rule requirements.

So I want to, I guess, emphasize that the 820.70(i) draft guidance that we're discussing today has a limited scope. And within that, we talk about a risk-based approach. The Part 11 guidance applies more broadly. And you might think of its validation requirements as something like what we're talking about for this draft guidance. But they are not the same. We're not talking about electronic records more broadly.

CDR Kim Piermatteo: Alright, thank you, Nellie, for that question. And thank you, Cisco and Ian, for those responses. Alright, our next question is coming from Charles. Charles, I've unmuted your line. Please unmute yourself and ask your question.

Charles Webb: Thank you so much. Everyone has a unique risk tolerance level-- individuals, companies, project teams. Is there a definitive, quantifiable right or wrong answer when taking the risk-based approach? I mean, is it possible that you can get a 483 if a team may have minimized the risk?

Cisco Vicenty: So I think-- and I just want to make sure that I'm putting into context. So if I'm misspeaking when I walk through this, please feel free to add more insight, or maybe somebody else on the team can also help correct. But when we talk about guidances in general, and anything that we issue, it's a set of recommendations, our current thinking. That isn't the reg, right? That's not what we are enforcing to.

So if there is a 483 issued, it isn't in reference to not following a situation in the guidance. There's something else that went on that was found to be in violation or an observation within what could potentially be a violation of the reg. The work here-- and we absolutely understand that the risk tolerance and the risk points vary. They're product-specific. As we talk about in this guidance, they could be process-specific. What we want to make sure is that it's clear to organizations that really you are the experts in your processes, in your risk. It should be in the product also. This gives you the flexibility to have that discussion about that risk and why you thought it was the appropriate determination.

CDR Kim Piermatteo: Thank you, Cisco, for that response. Alright, our next question is coming from Sarah. Sarah, I have unmuted your line. Please unmute yourself and ask your question.

Sarah Wilson: Yes, thank you very much. My question is really around the docket and the comments that are to be submitted on that docket. Is there a way for others to be able to have the ability to see what has already been submitted on the guidance within that docket or not?

CDR Kim Piermatteo: Thank you, Sarah. Mary, would you like to provide a response?

Mary Wen: Sure, and the answer is yes. Under regulations.gov, you will be able to see the comments that have been posted to the docket publicly. Thank you.

Sarah Wilson: Perfect. Thank you.

CDR Kim Piermatteo: Thanks, Sarah. Thanks, Mary. Alright, our next ques—

Ian Ostermiller: Hi, this is Ian Ostermiller. I just wanted to add a little step in there. The visibility for the public is not an automatic step. So our dockets management staff will review comments and make sure that it's not confidential information or something like that that's been appropriately marked according to the directions.

They're not making their own judgment calls. But they will first go through and look at the comments to make sure they can be made visible to the public. So it's not going to happen instantaneously. Our dockets management staff will review it.

Sarah Wilson: Thanks, Ian, for that clarification.

CDR Kim Piermatteo: Alright, our next question is coming from Antonio. Antonio, I've unmuted your line. Please unmute yourself and ask your question.

Antonio Agullo: Yes, hello. My question basically is, these guidances at now Section 6, I think, will be, I guess, nullified from the previous software violation guidance. My [INAUDIBLE] following that had a general statement-- because this went around off-the-shelf software, automated equipment, and so on-- that even though a least burdensome approach could be followed, we should still consider what was in the previous sections based on complexity. And I want to have a feeling for what you think about automated manufacturing equipment to assemble parts and whatnot that is custom for a company. Should we still consider the stuff above Section 6 for those computerized automated systems?

Cisco Vicenty: So I think we are talking about the automated equipment, especially customized for an organization, whether it is just simple configuration or you're fully automating all that pieces, that weights into your overall risk calculus and your risk determination. I think even in the general principles of validation guidance, in the previous portions that are referenced, they also still outline that consideration of risk when establishing the validation activities for things that are in-house custom developed on that end.

So I don't think that you're out of step in weighing that and adjusting and applying the overall methodologies and approach that are outlined in the broader guidance and in the work you're doing here. Even if it is a custom automated equipment piece, that's really part of what was intended within the broader 820.70(i) reg.

Antonio Agullo: Alright, thank you.

CDR Kim Piermatteo: Thank you, Cisco. Alright, I think we're going to have time for two more questions. Karen, I have unmuted your line. Please unmute yourself and ask your question.

Karen Reich: Hi. During the presentation, it was mentioned that audit trails are recommended. And I was wondering if you could provide additional advice or direction as to determine when an audit trail is recommended versus when it's not recommended or not needed.

CDR Kim Piermatteo: Thank you, Karen, for that question.

Cisco Vicenty: I think the idea with the scope of the audit trail is that it becomes an extra element that you weight in, again, with your risk evaluation, and your decision, and effort of activities selected to provide that assurance. Right, it becomes an extra-- just an extra information set to help establish that confidence base. While it's recommended if the system does it, I think what and how you use the audit trail, what gets captured really is dependent on your application and what the tool is doing. And then back to the points earlier, what's the risk that occurs, and where does it occur should the system not perform as intended?

If there's any more specific details regarding application, you can always reach out to us individually and discuss it. But I think we tried to leave that broad so that there's flexibility in what the manufacturers were applying or doing.

Karen Reich: OK. Alright, thank you.

CDR Kim Piermatteo: Thank you, Karen. Thank you, Cisco. We have time for one more question today. Our last question is coming from Rhonda. Rhonda, I have unmuted your line. Please unmute yourself and ask your question.

Rhonda: Hi. Thank you. The question is about validating COTS or OTS products. The tools that are in general use, such as Microsoft Word or Excel tool, if it's not being configured, it's just being used out of the box. In past life, we've written justifications as to why general use tool did not need to have a validation. Is that the same going forward, or do we need to go through the validation process and put the paperwork together if we're using Word, like I said, out of the box?

Cisco Vicenty: Yeah, and I think one of the examples in there was trying to make that point clearly. If you've got something that's out of the box, there isn't anything that's being configured and you're using it as it was intended to, I mean, there isn't a lot more that you can do in terms of validation. So when you start using that tool in a specific context, a specific set of features, you're developing, in the example, an Excel sheet that does its own set of calculations for a specific quality record. You're validating that specific sheet, that application, not Excel.

Rhonda: Excellent. Thank you so much.

CDR Kim Piermatteo: Thank you, Rhonda, for that question. And thank you, Cisco. And thank you, everyone, for a very engaging question and answer segment. At this time, I'd like to turn it back over to Cisco today for his final thoughts. Cisco?

Cisco Vicenty: Thank you, Kim. And thanks to everyone for the engagement and for really being part of what we are trying to get a better handle on, understand here. So as we've discussed here with the body of work here, a lot of it is intended to be a recommendation to really help out in addressing situations that we heard or current state of things for manufacturers. This is a process, and we are open to comments. So if there are specific feedback, improvements that could be made, things where we have in fact not considered, please take the time and put that information in the docket so that we can consider it, review, and make this a better, more useful product for everyone.

CDR Kim Piermatteo: Thank you, Cisco, for those final thoughts. And again, thank you for your presentation today on this draft guidance. I'd also like to thank Ian and Mary for their participation in today's webinar.

Please keep in mind, for those of you who are attending, printable slides of today's presentation are currently available on CDRH Learn at the link provided on the slide under the section titled Postmarket Activities and then the subsection titled General Policy. A recording of today's webinar and a transcript will be posted to CDRH Learn under the same section and subsection in the next few weeks. A screenshot of where you can find the presentation materials are provided on the slide.

If you have additional questions about today's webinar, please feel free to email us at DICE@fda.hhs.gov.

We also encourage you to attend a future CDRH webinar. A listing of all of our upcoming webinars is available at www.fda.gov/CDRHWebinar. This concludes today's CDRH webinar. Thank you all again for joining us and have a nice day.

****

END