**Quality Management System Regulation (QMSR) – Risk Management, Risk-Based Approach, and Risk-Based Decisions**

Slide 1

Hello, my name is Tonya Wilbon, Assistant Director for the Postmarket Industry Education Team and the Consumer Education Team of the Division of Industry and Consumer Education, in the Center for Devices and Radiological Health, at the U.S. Food and Drug Administration.

Welcome to CDRH Learn, FDA's preeminent catalog of multi-media educational modules about medical devices and radiological products. In this module, I will focus on the Quality Management System Regulation, hereafter referred to as QMSR, requirements for Risk Management, Risk-Based Approach, and Risk-Based Decisions.

Slide 2

This image illustrates the comprehensive nature of risk management throughout the product lifecycle, from initial design through postmarket surveillance. Some of you may think that the requirements pertaining to risk may look similar to this image; sketchy, crowded, uncertain, and even perhaps overwhelming. Hopefully this presentation, will provide you with knowledge, clarity, and resources to understand and successfully implement risk requirements of the QMSR.

Slide 3

This presentation has four key learning objectives. The learning objectives are: to define essential risk terms that form the foundation of this presentation; to explain the role of risk management within the broader Quality Management System; to identify the QMSR requirements for risk management, risk-based approaches, and risk-based decisions; and to review a few examples of risk documentation.

Slide 4

Let's begin by defining a few key terms used in this presentation.

Slide 5

Understanding key risk terms is crucial for implementing effective risk concepts in your quality management system. Risk is defined as the combination of the probability of occurrence of harm and the severity of that harm. This term describes what could go wrong, how likely it is to happen, and how serious the consequences would be.

Risk management is defined as the systematic application of management policies, procedures, and practices to the tasks of analyzing, evaluating, controlling, and monitoring risk. The term systematic used in the definition clarifies that this is a structured and documented approach to addressing risk.

These terms are defined in the American National Standards Institute, hereafter referred to as ANSI, the Association for the Advancement of Medical Instrumentation, hereafter referred to as AAMI, and the International Organization for Standardization, hereafter referred to as ISO, thus the ANSI/AAMI/ISO 13485:2016 Standard titled, "Medical devices-Quality management systems- Requirements for regulatory purposes" and the ISO Standard 14971:2007, titled, "Medical devices-Application of Risk Management to Medical Devices." As indicated in FDA's response to Comment nine, FDA does not, in this rulemaking incorporate ISO 14971 or any other standards referenced by, or listed as a source in, ISO 13485, but acknowledges that these other standards may be helpful in understanding application of ISO 13485.

Slide 6

FDA further clarified in their response to Comment 32 in the Final Rule that the definition of the term risk used by ISO 13485 is appropriate. Clause 0.2 in ISO 13485 states that, when the term risk is used, the application of the term within the scope of this International Standard pertains to safety or performance requirements of the medical device or meeting applicable regulatory requirements. FDA stated that it believes that a definition of risk unique to QMSR is thus not necessary.

Slide 7

Two additional key terms are risk-based approach and risk-based decision. Risk-based approach is defined as identifying risks and opportunities and focusing on preventing or reducing undesired effects. This is more of a proactive approach. Risk-based decision is defined as making a specific decision based on risk assessment and other criteria. The information obtained is actively used to drive decisions throughout the life of the device and throughout the quality management system.

Slide 8

Now let's explore the role that risk management plays within your quality management system.

Slide 9

Risk management serves several core functions. It helps identify, assess, control, communicate, and review device risks to the quality management system processes. It provides reasonable assurance of

safety and effectiveness throughout the total product lifecycle, from design and development through postmarket surveillance and eventually discontinuation.

Slide 10

Risk management provides a framework for sound decision-making within your quality management system. For example, it helps you identify which design outputs are essential for proper device functioning, guides continuous updates based on postmarket surveillance data, defines the extent of verification activities for purchased products, and determines the appropriate approach to software validation and revalidation activities proportionate to the associated risks with the use of the software.

Slide 11

Let's now examine the specific QMSR requirements for risk management, use of a risk-based approach, and making risk-based decisions.

Slide 12

Title 21 Code of Federal Regulations Section 820.10(a) requires manufacturers to document a quality management system that complies with applicable requirements of ISO 13485, along with other applicable requirements. ISO 13485 is incorporated by reference per 21 CFR 820.7 and includes specific requirements for risk management, risk-based approach and risk-based decision making. FDA clarified these requirements in their responses to Comments 19 and 27 in the 2024 Medical Devices Quality System Regulation Amendments, Federal Register Volume 89 page 7496 Final Rule referred to as 2024 Final Rule hereafter.

Slide 13

In their response to Comment 19, the FDA emphasized that while the integration of risk management principles throughout ISO 13485 doesn't represent a philosophical shift, the explicit integration throughout the clauses of ISO 13485 more clearly establishes requirements for risk management throughout the quality management system or QMS. This should help industry develop more effective total product lifecycle risk management systems. FDA emphasized in their response also that in adopting ISO 13485, the QMSR incorporates these risk concepts and principles as important elements of an effective quality management system.

Slide 14

In the FDA's response to Comment 27, FDA clarifies that it is the expectation for medical device manufacturers, led by individuals with executive responsibilities, to embrace a culture of quality as a key component in ensuring safe and effective medical devices. FDA also states that this culture of quality meets regulatory requirements through specific behaviors, attitudes, activities, and processes.

Slide 15

In adopting ISO 13485, QMSR incorporates risk management throughout its requirements and emphasizes risk management activities and making risk-based decisions. These requirements for risk management, use of a risk-based approach, and making risk-based decisions are included throughout multiple clauses of ISO 13485 including Clause 4.1 for General Requirements, Clause 6.2 for Human Resources guidance and understanding, Clause 7.1 for Planning of product realization requirements, Clause 7.3 for Design and Development requirements and Clause 7.4 for Purchasing requirements.

Slide 16

QMSR requirements for risk management, use of a risk-based approach, and making risk-based decisions are also included in Clause 7.5 for Production and service provision requirements, Clause 7.6 for Control of monitoring and measuring requirements, Clause 8.2 for Monitoring and Measurement requirements, Clause 8.3 for Control of nonconforming product, and Clause 8.5 for Improvement. Notice how risk management permeates throughout the quality management system.

Slide 17

Under Clause 4.1, General Requirements, organizations must apply a risk-based approach to control appropriate QMS processes. Controls must be proportionate to the risk involved and the external party's ability to meet requirements for outsourced processes. Additionally, software validation and revalidation activities must be proportionate to the risk associated with software use. For example, you can review your QMS and identify risks or areas of needed improvement within the processes using the method that best suits your needs such as use of Strengths, Weaknesses, Opportunities and Threats analysis or SWOT or even a simpler technique such as Brainstorming techniques. Once area of needed improvement is identified, you can then use a more detailed analysis such as Hazard, Analysis and Critical Control Points, HACCP, to create a plan for process improvement or implementing control measures.

Slide 18

Clause 6.2, Human Resources, includes a note for guidance that the methodology used to check training effectiveness should be proportionate to the risk associated with the work for which training is provided. For example, some low-risk job assignments, training could be limited to requiring the individual assigned to the job to read the content of procedures that describe the job assignment. Whereas higher-risk activities warrant more rigorous training verification such as testing or questioning the trained individual or even evaluating their work performance.

Slide 19

Clause 7.1, Planning of product realization, requires organizations to document one or more processes for risk management in product realization and maintain records of risk management activities. This ensures risk management is not just conceptual but documented and traceable. As indicated in the NOTE of this standard, ISO 14971 standard can be used to obtain further information pertaining to and for documenting risk management processes.

Slide 20

Under Clause 7.3, Design and Development, inputs must include applicable outputs of risk management and other requirements essential for design and development of the product and processes. Review and approve design and development inputs to ensure they are complete, unambiguous and compatible with each other, and thus conflicts are resolved prior to final approval of the inputs. Design and development outputs must specify characteristics of the product that are essential for safe and proper use.

Slide 21

In addition, Clause 7.3 specifies that when controlling design and development changes, reviews must include evaluation of effects on constituent parts, products in processes or already delivered, inputs or outputs of risk management, and product realization processes. The evaluation and documentation of the change should be in direct proportion to the significance of the change and communicated to relevant functions in your organization to determine the total effect of the change.

Slide 22

For Clause 7.4, Purchasing, criteria for supplier evaluation and selection must be proportionate to the risk associated with the medical device. The selection process and controls might differ when applied to a contract sterilizer, a supplier of off-the-shelf components, or a design and development service based

on the criticality of the process and product being provided to the safety and performance of your product as well as the adequacy or effectiveness of your QMS. When suppliers don't fulfill purchasing requirements, this is addressed proportionate to the risk associated with the purchased product and compliance with applicable regulatory requirements also.

Slide 23

Clause 7.4 also requires that the extent of verification activities for purchased products must be based on supplier evaluation results and proportionate to the risks associated with the purchased product. Higher risk purchased product or services require more extensive verification. It is the organization's decision regarding the appropriate type and extent of its control and evaluation activities.

Slide 24

Clause 7.5, Production and service provision, requires that for the validation of computer software used in production and service provisions, a specific approach and activities associated with software validation and revalidation be proportionate to the risk associated with software use, including effects on the product's ability to conform to specifications. Some processes require that operators have extra training or be specially qualified or that the process itself have a specific approval.

Slide 25

Similarly, Clause 7.6, Control of monitoring and measuring equipment, requires that for the validation of the application of computer software used for monitoring and measurement of requirements, a specific approach and activities associated with software validation and revalidation be proportionate to the associated risks and effects on product conformity to specifications. For example, a manufacturer uses software-based environmental monitoring to track temperature and humidity in cleanrooms where sterile syringes are assembled. This software directly affects the ability to meet product specifications, thus the company would be required to develop a validation and revalidation plan to ensure the software performs as intended.

Slide 26

Under Clause 8.2, Monitoring and measurement, information gathered through feedback processes must serve as potential input into risk management for monitoring and maintaining product requirements and product realization or improvement processes. For example, you reviewed several complaints received over a period of time and identified an increase in the frequency of the malfunction

of a specified part. The risk management file should be reviewed and updated accordingly and determined if the risk profile changes and if risk control measures are required.

Slide 27

Clause 8.3, Control of nonconforming product, requires that when nonconforming product is detected after delivery or use has started, organizations must take action appropriate to the effects or potential effects of the nonconformity. The response must match the risk level. This could include activities such as notifying customers, issuing field safety notices, conducting product recalls, or performing corrective actions to prevent recurrence.

Slide 28

Finally, Clause 8.5, Improvement, requires that corrective actions be proportionate to the effects of nonconformities encountered, and preventive actions be proportionate to the effects of potential problems. The degree of action taken should be dependent upon and related to the risk. For example, you may decide to recall and relabel the device with misprinted instructions as a corrective action for a high-risk device or you may add extra validation checks before a software update rollout as a preventive action for a high-risk device.

Slide 29

Now let's look at a few examples of risk documentation of these requirements.

Slide 30

This slide lists two resources that contain useful information regarding risk management activities and documentation. The AAMI/ANSI/ISO 14971:2019 standard, titled Medical device Application of risk management to medical devices which provides a systematic approach to conducting risk management activities, and the AAMI/ISO TIR24971:2020 document, titled, Medical devices guidance on the application of ISO 14971, which provides guidance on applying ISO 14971.

Slide 31

There are several ways in which you can document your risk activities and decisions as depicted on this slide and the subsequent slide. You can use a Risk Management Plan which outlines the risk management scope, responsibilities, and criteria at the start of product development. You can use a Risk Analysis Report to identify hazards and estimate risks during design and development. Some individuals capture their risk information using a Risk Evaluation Summary to document the justification of the

acceptability of individual and overall risk. A more popular example for documenting risk information is by use of a Risk Traceability Matrix which demonstrate that risks are addressed and mitigated throughout the product lifecycle. And then there is the Risk Management File which serves as a centralized record of all risk-related documentation maintained throughout the device lifecycle.

Slide 32

Additional examples of risk documentation include Design Review Meeting Minutes, Change Control Records, Improvement Documentation, Production and Process FMEAs, and Benefit-Risk Analysis Report.

Slide 33

This slide list a few key resources referenced in this presentation, including the 2024 Final Rule, ISO standards, and specific guidance documents. These references will help you access the detailed requirements and guidance mentioned during this presentation.

Slide 34

In summary, risk management is integral to safe and effective devices and an effective quality management system. The QMSR incorporates risk management principles, risk-based approaches throughout the total product lifecycle, and incorporates risk-based decision making within the QMS by incorporating by reference ISO 13485:2016.

Slide 35

The Division of Industry and Consumer Education provides you with regulatory education in several key formats, so you can choose the most effective way you wish to learn. CDRH Learn consists of over 200 multi-media industry education modules, such as the one that you are viewing here. These include videos, webinars, presentations, and various “how to guides.” Use your computer, phone, or portable device to click on the link shown here. Now, if you prefer to learn by reading, check out Device Advice. Device Advice consists of several hundred pages of comprehensive regulatory information across the device total product life cycle. And finally, if you have a specific question and wish to ask us directly, I encourage you to call or email us using the contact information located on this slide.

Slide 36

Let's conclude this module with your call to action. First, review the QMSR requirements for risk management, risk-based approaches, and risk-based decisions. Document your risk management

activities thoroughly and revisit them frequently. And finally, use risk management as a framework for sound decision-making within your QMS to provide assurance that your devices will be safe and effective.

Thank you for your attention to this module, Quality Management System Regulation, QMSR, Risk Management, Risk-Based Approach, and Risk-Based Decisions.

**********