Global Harmonization Working Party

GHWP

Towards Medical Device Harmonization

FINAL DOCUMENT

Title: **Guidance Document on the Risk-Based Approach to Quality Management System Aspects: ISO13485:2016**

Authoring Group: Working Group 7 – Quality Management System - Operation and Implementation

Date: [25 Nov, 2023]

Dir. Chen Yan

Chair, Working Group 7

Mr. Liew Ee Bin

Co-Chair, Working Group 7

Table of Contents

Preface

The document herein was produced by the Global Harmonization Working Party (GHWP), a voluntary group of medical device regulators and industry from GHWP member countries in Asia and beyond. The document has been subject to consultation throughout its development.

Introduction

The 'risk-based approach' as required by the ISO13485:2016 standard is represented by the phrase "proportionate to the risk" and it appears 10 times in the standard's text. With the release of the ISO13485:2016 standard, there had been confusion with regards to determining this risk-based approach, its practical implementation in the relevant quality system aspects and the differences in application with ISO14971:2019 standard.

This guidance document aims to provide practical suggestion and clarity on the approach, improve compliance to standards and regulations, and to save on unnecessary allocation of resources by the industry and regulatory authority, improve overall patient safety.

Note that there is no requirement in the ISO 13485:2016 standard to use formal risk management in the identification of risks within the QMS processes themselves, but it is the implementation of a risk-based approach within the processes that is outlined. That said, this guidance document provides suggestions for the practical implementation of the risk-based approach.

Purpose

This document is to provide the general principles of quality management system considerations with regards to the tasks and deliverables necessary to provide specific guidance for the risk-based approach and its practical implementation in ISO13485:2016.

This guidance document provides the various methodologies and techniques to apply the risk-based approach correctly in the following quality management systems aspects:

1. Competence assessment of human resources
2. Supplier management and outsourcing processes
3. Computer systems (software) validation relating to the QMS and production processes.
4. Corrective and Preventive Actions (CAPA), and Post-Market Activities

Scope

This document applies to applicable medical devices and IVD medical devices intended to be marketed in to regulated countries, or manufactured in regulated countries.

References

- ISO 13485:2016 - Medical devices — Quality management systems — Requirements for regulatory purposes
- ISO 13485:2016 - Medical Devices - A Practical Guide
- IMDRF MDSAP Audit Approach Document No: MDSAP AU P0002.005
- IMDRF / GHTF Quality Management System – Medical Devices – Guidance on the Control of Products and Services Obtained from Suppliers

1 Definitions

1.1 Risk

Combination of the probability of occurrence of harm and the severity of that harm

Note 1 to entry: This definition of “risk” differs from the definition given in ISO 9000:2015.
The term "risk" in ISO 9000:2015 refers to uncertainty for the organisation, whereas in ISO 14971, the same term is referring to potential harm being caused by or during the use of a medical device.

[SOURCE:ISO 14971:2019, 2.16]
[SOURCE:ISO 13485:2016, 3.17]

1.2 Risk-Based Approach

To identify uncertainty in the organization’s processes, and to apply controls within the appropriate processes to mitigate potential negative effects and maximize potential positive effects.

2 Integration of the Risk-Based Approach in the Quality Management Systems

A risk-based approach allows flexibility in actions based on an organization’s risk tolerance and helps an organization make balanced decisions.

There are many actions that your organization can take to address risk and these are often covered by requirements in ISO 13485. Some examples, include, but not limited to:

- defining responsibilities and authorities, and its extent
- identifying training needs, implement training and assigning competent persons.
- documenting specified methods and work instructions to the required level of detail
- implementing inspection or other monitoring and measuring of processes and product.
- implementing varying process validation techniques
- calibration frequency of measuring and monitoring devices.
- implementing corrective actions and making sure that these are appropriately extended to other relevant areas of your organization.

Quality management system aspects are inter-related and inter-dependent. Figure 1 explains the inter-relationship between various quality aspects, and the activities in which its extent and frequency is proportionate to the risk associated with that process.

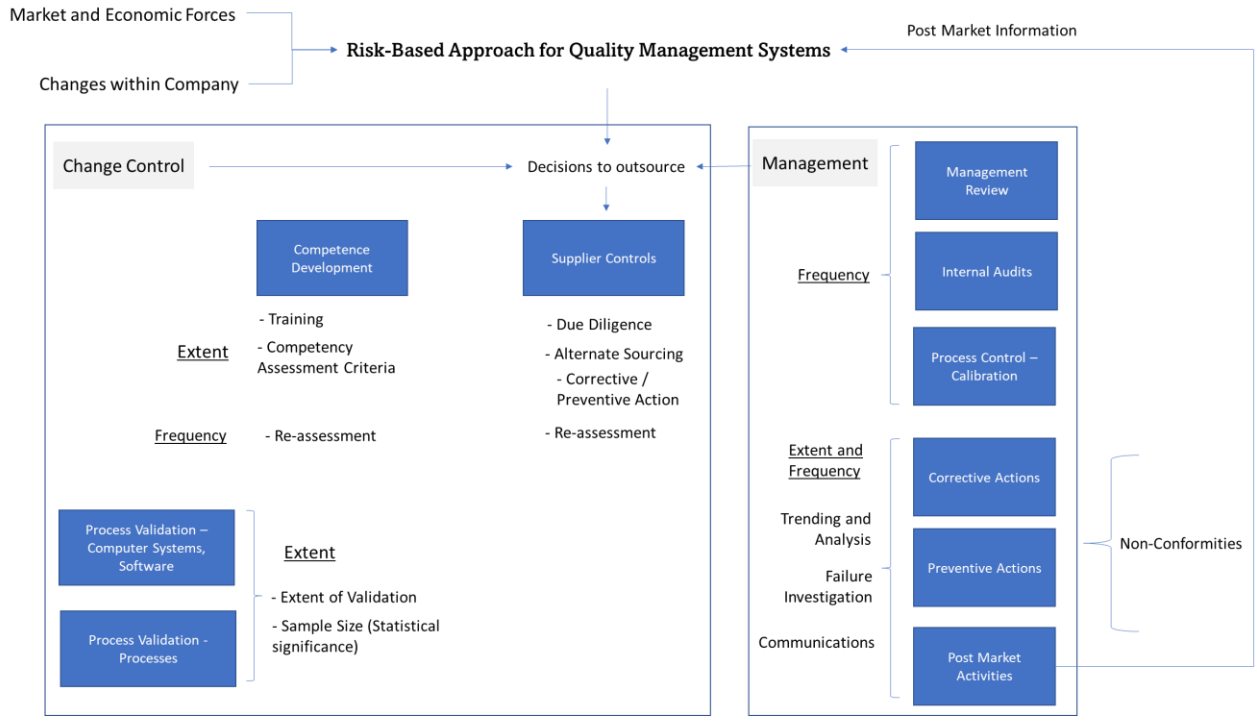

Figure 1 - Inter-relationship between quality system aspects implementing the risk-based approach to the quality management system.

Navigating the Risk-Based Approach in the ISO1345 Standard

Clause 4.1.2 mandates that "The organization shall apply a risk-based approach to the control of appropriate processes needed for the quality management system."

The quality management system can be impacted by external factors such as investment inputs, share price in the stock markets, market forces such as changes in government policies, availability of components, supply chain, and internal changes such as succession planning, cost-down, improvements in organisational efficiency.

Sections within the ISO 13485:2016 standard specify risk considerations that need to be addressed in the appropriate processes within the QMS, for example:

- method to determine the effectiveness of training of personnel (6.2)
- decision to outsource processes (4.1.5), method of selection and monitoring of suppliers (7.4.1) , extent of verification of purchased product (7.4.3)
- extent of validation, including validation of software (4.1.6, 7.5.6, 7.6)

Additional examples of the application of the risk-based approach where ISO 13485 does not specifically outline risk considerations:

- interval for management review (5.6) and internal audit (8.2)
- control of production, service, and calibration of measurement equipment (7.5.1, 7.6)
- disposition of nonconforming product and nature of correction necessary (8.3)
- determination of actions to prevent occurrence or recurrence of nonconformities (8.5.2, 8.5.3)

In essence, the risk-based approach is an organisations' judgement on the risk of a process, a service, or a situation, in relation to product safety, quality, compliance, and the quality management system, then apply an appropriate method to manage these risks.

3 Methods Pertaining to the Risk-Based Approach to Quality Management System Aspects

3.1 Introduction

Simple processes might require only simple explanations. Complex processes will require sufficient explanation to enable your people to understand the activities and tasks, and the inter-relationships, to the extent necessary to implement their roles effectively. Some processes may require less frequent checks as it is a stable or it is further away from impacting product quality/compliance, some would require more frequent verification if the variation is likely to be high.

The explanation simply describes the key methods of applying the risk-based approach:

a. The **extent** of the activity – verification, evidence of meeting an objective, the level of the customer requirement, direct roles and responsibilities

b. The **frequency** of these activities

c. A **combination of varying the extent and frequency**

Risk-based approach does not equate Risk management. While ISO 13485 does not require formal risk management in identification of risk at the QMS level, Clause 7.1 requires you to document a process or series of processes for risk management in product realization. This relates to risk management in regards to the safety and performance of the medical device from design and development through post-production activities. ISO 14971 provides specific information on product risk management for medical devices.

With respect to Figure 1, the application of the risk-based approach on the Various Aspects of the Quality Management System is described in the following sections.

3.2 Risk-Based Approach for the Quality Management System

Applicable Clauses

4.1.2 The organization shall:
…..
b) apply a risk based approach to the control of the appropriate processes needed for the quality management system;
c) determine the sequence and interaction of these processes.
…. Basis for risk-based approach and management of these processes

4.1.5 When the organization chooses to outsource any process that affects product conformity to requirements, it shall monitor and ensure control …. controls shall be proportionate to the risk involved and the ability of the external party to meet the requirements in accordance with 7.4…

Applying the risk-based approach within the organisation

The documentation for a risk-based approach can be informal (discussion and brainstorming) or formal (structured approach). It is not expected for an organisation to develop a document to describe the risk-based approach to the quality management system aspects, but to include them in various process procedures and guidelines.

Decision to Outsource

The decision to outsource depends on managements determination of risk to the product quality/compliance and quality management system. This in turn is impacted by the organisation's available resources and various internal/external factors.

For example, which components / software are produced by the organisation, which are produced by 3rd-party suppliers. Which resources are outsourced (for example, logistics, administration) and which must be insource (for example, design and development, sales). It is important to emphasize that quality responsibility cannot be outsourced, as the organisation needs to be ultimately responsible for the quality of the medical device.

Note: See section on Supplier Controls

Summary

Decisions to outsource is based on available resources within the organisation, these decisions are recommended to be documented.

3.3 Management Review, Internal Audit

Suggested risk-based approach – varying frequency.

The management review and internal audit requirements are clear and unambiguous. The frequency of these activities may vary from organisation to organisation. Management review can be impacted by the physical locations of the management team and the size of organisation. Internal audit can be impacted by the complexity of organisation.

Usually there is a rule of thumb of at least one review per year, and one internal audit per year, but the occurrence of the management review and internal audit can increased due to the expected growth or change of the organisation. Some management review may be triggered by market forces or internal organisation change (for example, change in executive management, change of ownership). Some internal audit may be triggered by personnel change, or integration with another organisation (for example, an acquired business with a different quality system)

3.4 Validation

3.4.1 Computer Systems, Software

Applicable Clauses

4.1.6 The organization shall document procedures for the validation of the application of computer software ….The specific approach and activities associated with software validation and revalidation shall be proportionate to the risk associated with the use of the software.

Suggested Risk-based approach - Extent of Validation

The extent of software validation depends on:

- Where the software / computer systems are implemented, with regards to the product quality/compliance, and the quality management system

- To what extent is the software / computer systems coded/configured by the organisation (as compared to having the code/configuration done by the software vendor)

There is a range of software validation techniques and extent of validation, A lower-risk software that is a commercial off-the-shelf (COTS) software (such as a CRM that does not store product traceability records) would require a validation for use and obtain a validation report from the vendor. A software that impacts the quality system and is configured by the organisation (for example, some of the eQMS software, ERP), would require system integration tests, and validation of the software requirements specifications (SRS). Further examples include software used for process automated detection of nonconforming product will require a more extensive validation, or using Microsoft Excel for record keeping, for process control, for determination of priority in CAPA.

It is useful to consult resources such as ISO/TR 80002-2 (validation of software for medical device quality management system), Good Automated Manufacturing Practices (GAMP) and ISO 10012 (Requirements for measurement processes and measuring equipment). As technology becomes

an increasingly important aspect of medical device design and manufacturing, software validation needs to be an area of focus in your QMS. Another emerging area is software used for mitigation of cybersecurity risks, which also needs to be adequately validated to meet rapidly changing regulatory requirements.

Summary

Software Validation
Software used in QMS, production, and service provision, monitoring and measurement – the specific approach and activities associated with software validation and re-validation shall be proportionate to the risk associated with the use of the software

- Assess risk to the final product quality/compliance
- Establish acceptance criteria
- ISO/TR 8002-2, GAMP, ISO10012
- Establish procedures and maintain records

3.4.2 Validation - Processes for Production and Service Provision

Applicable Clauses

7.5.6 Validation of processes for production and service provision

The organization shall validate any processes for production and service provision where the resulting output cannot be or is not verified by subsequent monitoring or measurement and, as a consequence, deficiencies become apparent only after the product is in use or the service has been delivered.
Validation shall demonstrate the ability of these processes to achieve planned results consistently.
….
d) as appropriate, statistical techniques with rationale for sample sizes
f) revalidation, including criteria for revalidation; …

Suggested Risk-based approach – Extent of the statistical significance.

The method of applying statistics can vary depending on the criticality of the process creating the product/component. While the decision to execute process validation and the methods of scientific examination can be determined by the criticality of the product/component, the statistical significance (acceptable quality level, the confidence level) varies according to the organization. While there may be rule of thumb (95% acceptable/95 CI, 99% acceptable/95% CI), this significance needs to be proportionate to the criticality of the part or the process.

3.5 Control of monitoring and measuring equipment

Applicable Clauses

7.6 Control of monitoring and measuring equipment
The organization shall determine the monitoring and measurement to be undertaken and the monitoring and measuring equipment needed to provide evidence of conformity of product to determined requirements. ….
In addition, the organization shall assess and record the validity of the previous measuring results when the equipment is found not to conform to requirements. The organization shall take appropriate action in regard to the equipment and any product affected. ….

Suggested Risk-based approach – Frequency of Calibration

For measurement equipment calibration, the calibration frequency can be increased or decreased – as long as it does not go beyond the minimum calibration frequency as recommended by the equipment manufacturer, depending on the process control data

3.6 Competence Development

Applicable Clauses

6.2 Human resources
Personnel performing work affecting product quality shall be competent on the basis of appropriate education, training, skills and experience.
…
The organization shall:
a) determine the necessary competence for personnel performing work affecting product quality;
b) provide training or take other actions to achieve or maintain the necessary competence;
c) evaluate the effectiveness of the actions taken.
….
e) maintain appropriate records of education, training, skills and experience (see 4.2.5).

NOTE The methodology used to check effectiveness is proportionate to the risk associated with the work for which the training or other action is being provided.

Suggested Risk-Based Approach

- Extent of pre-existing Knowledge, Experience
- Extent of Training; type of training
- Extent of Competency Criteria
- Frequency of Re-assessment

Clause 6.2 of ISO13485:2016 focuses on competence of personnel, which is based on the 4 pillars of education, training, skills, and experience. In this context, the term competence implies demonstrated ability to complete a task and produce expected results.

Pre-existing Knowledge, Experience

Your organization also needs to maintain records of personnel competence. This includes the records of actions taken or training a person has received and results of the action that contribute to the evidence of competence. The records to show that the action or training course has been successfully completed and that competence has been achieved can be as simple or complex as necessary.

Extent of Training, Type of Training

The method for evaluating competence is proportionate to the risk of the job. At their simplest, the records consist of list of procedures with a signature or initials to confirm that personnel self-assessed their competence to use certain equipment, carry out specific processes or follow certain procedures. The records should include a clear statement that a person is now deemed to be competent to do the task they intend to perform. The effectiveness of any further action, education or training should be re-evaluated, after a period, to confirm that the competence achieved is maintained.

Competency Criteria

The competency criteria depends on the criticality of the task, which in turn may depend on the critical-to-quality requirements. For example, if it is the (manual) visual inspection of solder in a printed circuit board, it would require the inspector to be independently accredited. In the example of a newly-joined employee in the design and development team, other than the employee's experience and talent, an organisation may assign a mentor to learn the practical nuances of the design and development process in relation to project management. On the other hand, some document error that does not impact the overall understanding of a process may just have a 'read and acknowledge' instruction. Therefore, it depends on the nature of the task involved.

Re-assessment

If skills may be eroded (the ability to judge the quality of a solder) due to various factors (physical deterioration), or when there are new tasks or revised tasks, it would depend on the type of tasks that would determine the extent of the re-assessment of competency. Usually, the best practice is to indicate this re-assessment criteria, along with the competency criteria

Summary

Methodology to check effectiveness is proportionate to the risk associated with the work for which the training or other action is being provided.

- Assess risk of not adequately performing task – product safety/performance, compliance
- Build risk-based competence matrix – education, training, skills, experience.
- Achieve and maintain competence.
- Establish procedures and maintain records.

3.7 Supplier Controls

Applicable Clauses

7.4.1 Purchasing process
The organization shall document procedures (see 4.2.4) to ensure that purchased product conforms to specified purchasing information.
The organization shall establish criteria for the evaluation and selection of suppliers. The criteria shall be:
…..
d) proportionate to the risk associated with the medical device.
The organization shall plan the monitoring and re-evaluation of suppliers. ….
Non-fulfilment of purchasing requirements shall be addressed with the supplier proportionate to the risk associated with the purchased product and compliance with applicable regulatory requirements.

7.4.3 Verification of purchased product
…. establish and implement the inspection or other activities necessary for ensuring that purchased product meets specified purchasing requirements. The extent of verification activities shall be based on the supplier evaluation results and proportionate to the risks associated with the purchased product.
…. becomes aware of any changes …
…. organization or its customer intends to perform verification at the supplier's premises…

Suggested Risk-Based Approach:

- Extent of due diligence
- Extent of Supplier Controls
- Alternate sourcing
- Extent of corrective / preventive action
- Extent and Frequency of Supplier Re-assessment

<u>Due Diligence</u>

Due diligence refers to the systematic and objective investigation or an audit of a potential investment a business should take before entering into an agreement or a transaction with another business.

For example, the extent of due diligence of a supplier can be considered as a risk-based approach to supplier qualification. For example, depending on the criticality of the supplier, the due diligence activity can be an on-site or off-site, the level of detail of the evaluation checklist, how many functions are included in the evaluation, are there interviews with the team members of the supplier, if yes, how many.

Extent of Supplier Controls

All components would go through a risk management process to determine the impact of risk of failure. For example, criteria used to evaluate and select a third-party manufacturer of a critical part/raw material or sterilization process will need to be more rigorous than other non-critical items and/or processes. You may require them to have an ISO 13485 certified QMS, or ask for data to demonstrate high capability for critical safety and performance related parameters. Questions related to their reputation, business stability, credit rating etc. may also be relevant.

For example, software developers may develop a functional part of the code, GUI of the software, in which the degree of supplier controls would be correspondingly different (the level of detail of supplier auditing, for example)

These activities may range from accepting on certificate of analysis (COA) to sampling to 100% inspection. In practice, it may be challenging to install 100% lot inspection, and audit the suppliers every year, as the sheer number may be overwhelming. Furthermore, the supplier may not allow the device company to access all the time. On the other hand, not monitoring critical suppliers just because they are in a different geographical region is not acceptable.

Analysis of previous inspection data or customer complaints that may relate to purchased products may also be a factor in frequency and intensity of verification activities. History of responsiveness to nonconformances, supplier corrective action requests (SCAR) and effectiveness of implemented corrective/preventive actions may be mitigating factors.

Alternate Sourcing

Alternative Sourcing is usually acknowledged to be required as part of good supply practice. However, the reality is that typically the medical device company orders a relatively small quantity and therefore having challenges to qualify new sources as these sources may be unwilling to undertake the efforts and resource to be a medical device supplier. Therefore the suppliers for critical components within a medical device would be the important for the organisation to take steps to actively source for another supplier of the critical component. The extent of this effort is based on the risk of the component or process.

Supplier corrective / preventive action

See Section 3.8 on Post Market Activities and CAPA

Reassessment

Suppliers, are just like any company, it can change, be subject to market forces, and are directly impacted by supply chains. Upon the qualification of the supplier, while the criteria for re-evaluation is determined by the type of input or change, the frequency and level of detail of the re-assessment depends on how critical the supplier is to the organisation.

Summary
Outsourced Process – controls shall be proportionate to the risk involved and the ability of the external party to meet requirements

Supplier Evaluation and Selection – Criteria shall be proportionate to the risk associated with the medical device

Purchased Product – Verification: extent of verification activities shall be used on supplier evaluation results and proportional to the risk associated with the purchased product

- Assess risk to processes affected by supplier
- Assess risk final product quality/compliance
- Implement written quality agreement
- Develop and implement measurable criteria
- Establish appropriate controls – can range from supplier audits to lot sampling to 100% inspection
- Consider complaints and past performance
- Consider frequency and type of changes
- Establish procedures and maintain records

Company can consider a mixture of on-site, off-site audits, setting up process key process indicators (KPIs) for product quality / compliance, and on-time delivery, with an on-site audit every year for the top 10-15 critical component suppliers.

3.8 Post Market Activities and CAPA

Applicable Clauses - CAPA

8.5.2 Corrective action
The organization shall take action to eliminate the cause of nonconformities in order to prevent recurrence. Any necessary corrective actions shall be taken without undue delay. Corrective actions shall be proportionate to the effects of the nonconformities encountered.

8.5.3 Preventive action
The organization shall determine action to eliminate the causes of potential nonconformities in order to prevent their occurrence. Preventive actions shall be proportionate to the effects of the potential problems.

Suggested Risk-Based Approach:
- Extent of failure investigation
- Extent/frequency of communication
- Extent of trend analysis

For example, in the event of a product complaint, the effort to obtain complaint information (e.g. the number of attempts, methods to recover complaint information) should be proportionate

with the risk associated with the complaint. The extent (how detailed, and comprehensive) of the failure investigation is also proportionate with the risk associated with the complaint.

Once the investigation is complete and root cause found, the corrective and preventive actions can be developed based on this investigation and root cause.

Note:

Requirements for corrective and preventive actions, due to internal non-conformity or product complaints, is **not** risk-based as the corrective and preventive actions must be executed and effective to prevent recurrence.

Adverse trends found through trend analysis is not risk-based as the organization should follow the escalation steps as defined. However, the determination of the parameter limits can be risk-based if the trend is not product related (in which the outputs of the trend analysis is part of the risk management process per ISO14971:2019)

3.9 Utilizing the Risk-Based Approach in the Change Control Process

The change control process itself is a defined process where the criteria for change control is determined by the type of change. These changes can be impacting various aspects of the quality management system. Therefore the change control process would indirectly be adopting the risk-based approach

4 Conclusion

A risk-based approach can help an organization in:

- Supporting preventive actions
- Getting things right the first time
- Prioritizing resources, and
- Sustaining a robust quality process
- Assign actions and controls, set priorities based on the impact of the possible consequences to the organization.

Evidence of a risk-based approach can be found in an organization's explanation for decisions around prioritization, planning, and control measures.

When thinking about implementing these risk-related requirements, keep in mind that risks evolve as new information becomes available through post-market surveillance. Your Quality Management System needs to be sufficiently resilient to respond to these rapidly evolving risks. There needs to be a mechanism to identify, assess and respond to new risks and/or to changes in the level of existing risks in terms of severity and probability of undesired effects. New controls may need to be implemented, or existing controls may need to be adjusted.

If the Quality Management System is designed using a process approach, with clearly defined processes and their interaction, it may be more resilient to changes in the risk profile of your products and regulatory requirements. The emphasis on planning throughout the current revision is intended to promote a more thoughtful, risk-based approach for maintaining the integrity and effectiveness of your Quality Management System.

- END OF DOCUMENT -