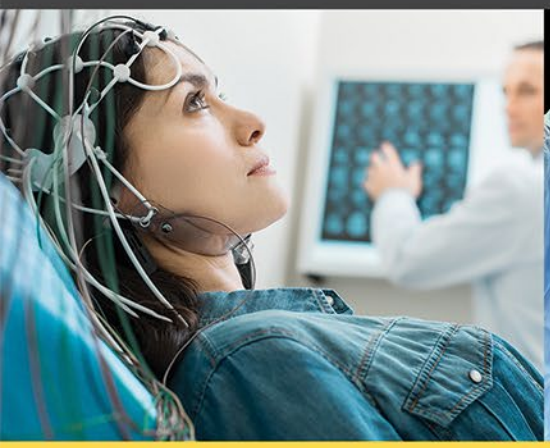
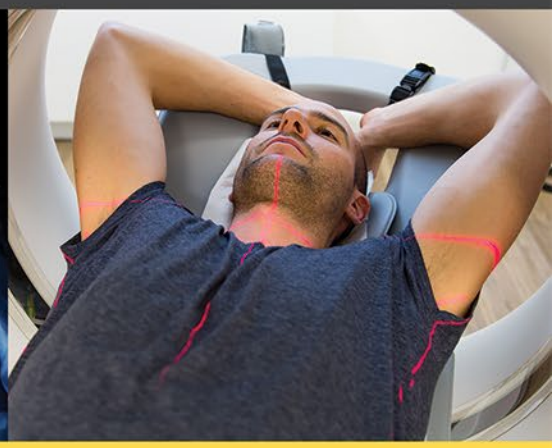
# ISO 13485:2016 & Risk-Based Approach

## An overview of new risk requirements and considerations for device manufacturers





**Author**
Alexandre Pétiard
EMERGO
Senior Consultant, QA/RA
apetiard@emergogroup.com

EMERGO
a UL company

September 2017

The ISO 13485:2016 and EN ISO 13485:2016 quality management system (QMS) standards have been published respectively in March and April 2016. Though they have not been formally recognized worldwide, the standards should be applied in the very near future. Manufacturers will have to be prepared for the transition by March 2019. The revised ISO 13485 standard is more aligned with US FDA 21 CFR part 820 and includes various updates (such as Medical Device File), refined requirements in design control (e.g., design verification, design validation, design transfer), and the addition of new procedures (e.g., Management Review Procedure). However, one of the main differences is the implementation of a risk-based approach for most of the QMS processes.

"The organization shall apply a risk-based approach to the control of the appropriate processes needed for the quality management system." (section 4.2.1)

## Concept

The ISO 14971:2007 and EN ISO 14971:2012 standards outline the risk management process necessary to mitigate the risks that may occur during the medical device life cycle (i.e., from design to removal). However, though ISO 13485:2016 fully includes ISO 14971 in its risk-based approach, these risk-based expectations are now extended to the QMS through which the medical device is developed and monitored throughout its life cycle.

The concept of risk is defined by ISO 13485:2016 as "safety or performance requirements of the medical device or meeting applicable regulatory requirements."

As a result of the new requirements established by the acceptance criteria, decisions regarding prioritization of tasks should now be defined based on:

- The ability of the medical device to meet the claimed level of safety or performance
- The ability to meet regulatory requirements

The main questions for manufacturers, contract manufacturers or suppliers who implement a QMS compliant with ISO 13485:2016 should include:

- How the risk-based approach should be documented in the procedures
- How the risk-based approach should be documented for companies producing various types of medical devices with a different level of safety or regulatory requirements
- How the risk-based approach will be applied every day when a decision is required

Though no rules are currently recognized as the state of the art and several years of Notified Body feedback will be necessary to take a strong position, the processes requiring a risk-based approach will have their procedures updated to include justified acceptance criteria based on medical device safety/performance and regulatory requirements. In addition to procedure updates and for day-to day-application, manufacturers will also need to update quality forms to include new/modified sections to capture specific documentation of results, actions, decisions, etc., against the acceptance criteria.

This risk-based approach concept will require an update or a new acceptance criteria definition and a deeper documentation of decisions, actions, and prioritization.

The next sections will detail the changes required by the standard along with some suggested updates in regards to the risk-based approach.

# Process Requirements

The following table presents processes that require an update to comply with the ISO 13485:2016 standard, as well as a proposed method to take the risk-based approach into account:

**Table 1: Summary of changes associated with Risk-based Approach (RBA)**

| Process | Paragraph | Main Changes | Proposed RBA |
|---|---|---|---|
| Control of appropriate processes | 4.1.2<br>4.1.5 | Apply a risk-based approach to the control of the appropriate processes needed for the quality management system; | • Document the regulatory, safety, and performance requirements for each process.<br>• Define indicators for all processes considering :<br>» each process must meet the regulatory requirements;<br>» the outputs of each process must be safe and efficient.<br>• Document suitable acceptance criteria to meet regulatory requirements as well as process safety and effectiveness. |
| Outsourced processes / Supplier Control | 4.1.5<br>7.4.1 | The organization should select, evaluate its suppliers (including subcontractors, consultants), and implement a suitable amplitude of actions necessary when the supplier does not meet the acceptance criteria defined. | • Define acceptance criteria of supplier evaluation.<br>• Define acceptance criteria of supplier selection.<br>• Define amplitude of actions according to acceptance criteria. |
| Software validation | 4.1.6<br>7.5.6 | The amplitude of software validation should be proportionate to risk when the software does not meet its specification. | • Define acceptance criteria to classify the software.<br>• Define the amplitude of evidence necessary, according to the software classification. |
| Human resource | 6.2 | Effectiveness of training should be evaluated through a method proportionate to the risk if the training was not conducted. | • Define acceptance criteria to classify each training.<br>• Define a training effectiveness review method according to the training classification. |
| Product realization | 7.1 | A process of risk management should be described throughout the product realization. | • Define a process/procedure of risk management according to ISO 14971 |
| Design change | 7.3.9 | The significance of all changes to function, performance, usability, safety, and applicable regulatory requirements for the medical device and its intended use must be determined. | • Update the design change form to include the evaluation of change impact for function, performance, usability, safety, and applicable regulatory requirements. |

# Process Requirements

| Table 1: Summary of changes associated with Risk-based Approach (RBA) | | | |
|---|---|---|---|
| **Process** | **Paragraph** | **Main Changes** | **Proposed RBA** |
| Incoming inspection | 7.4.3 | The incoming inspection (e.g., documentary review, visual control, tests) implemented should be proportionate to:<br>• risk associated with the purchased product;<br>• results of supplier evaluation. | • Evaluate the purchased product in the risk management process according to ISO 14971.<br>• Include the possibility to increase the amplitude of control after each supplier evaluation. |
| Measuring equipment | 7.6 | All software used as part of measuring equipment, should be validated and revalidated in a manner proportionate to the risk to the product to be out of specifications. | • Define acceptance criteria to classify software used as part of measuring equipment.<br>• Define the amplitude of evidences necessary according to the software classification. |
| Monitoring and measurement | 8.2.1 | The post-market surveillance should be input of risk management process, product realization, and CAPA process when necessary. | • The PMS should induce a review of risk management activities. |
| Audit | 8.2.4 | The audit program should be based on the importance of each process and the status evaluated at the previous audits. | • Establish a table of audit frequency according to process importance, status, and results from previous audits. |
| Field Safety Action | 8.3.3 | When nonconforming product is in use, risk evaluation should be done to determine the appropriate action plan. | • Define acceptance criteria to classify the level of risk for the NC product in use (based on ISO 14971 standard).<br>• Define amplitude of actions necessary according to the level of risk associated with the NC product in use. |
| CAPA | 8.5.2<br>8.5.3 | Corrective/Preventive actions should be proportionate to the effects of the nonconformities encountered. | • Define the acceptance criteria to classify all CAPAs according to risk or effect associated with the NC.<br>• Prioritize the CAPA according to its classification.<br>• Adapt the targeted timeline according to the CAPA classification. |

***Source**: Emergo*

*Note: The risk-based approaches already discussed in ISO 13485:2003 (e.g., evaluation of adverse effect following a rework, risk management is an input of design input) are not addressed in this paper.*

# Ensuring Compliance - Processes and Supplier Control

This section addresses manufacturers and sub-contractors integrating the ISO 13485:2016 risk-based approach into their QMS. However, the suggested tools must be considered carefully as they are only intended to give some principles and examples to address the new requirements.

## Control of appropriate processes / outsourced processes

Manufacturers may apply process controls through a risk-based approach by defining appropriate indicators and acceptance criteria to review the effectiveness of each QMS process. Those indicators and acceptance criteria may be reviewed for suitability and relevancy during the management review. As part of the QMS, manufacturers must control the outsourced processes (e.g., complaint handling, subcontractors) similarly with appropriate indicators and acceptance criteria to ensure efficiency of those processes.

The organization may document the definition of indicators, as well as their acceptance criteria considering that the process must comply with regulatory requirements, and that the process outputs must be safe and effective. The table below is an example of how to document this evaluation:

**Table 2: Example of process indicator management**

| Processes | Risks | | Indicators | Acceptance criteria | Rationale for acceptance criteria | Status the previous year |
|---|---|---|---|---|---|---|
| Corrective and Preventive Action (CAPA) | Regulatory requirements | 21 CFR part 100 | CAPA investigation | 100% of CAPA are investigated or justified when no investigation is implemented | No tolerance, all CAPA must be investigated | 90% |
| | | 21 CFR part 806 | FSCA reporting to authorities | 100% of FSCA are reported to authorities 10 days after the correction initiation | No tolerance, all FSCA must be reported within the required timeline | 100% |
| | Safety | Field Safety Corrective Action | FSCA initiation | 90% of FSCAs are implemented within the first month before being aware of the problem | In 2016, 60% of FSCA were implemented within 1 month after being aware of the problem and the organization wants increase the process effectiveness to reduce the safety risks | 60% |
| | Performance | CAPA treatment | Treatment duration of minor CAPA | 75% of minor CAPA are implemented in 1 month | The organization does not consider the minor CAPAs that remain open for more than 1 year in 60% of cases. | 20% |

***Source**: Emergo*

Example of indicators may be:

- For meeting the regulatory requirements: time from the complaint receipt to complaint reporting to FDA (< 30d); time from the complaint receipt to complaint reporting to FDA for public health risk (< 5d); time for reporting in EU a death or unanticipated serious deterioration in state of health of patient (<10d); % of CER made according to the targeted date – every year (100%).
- For ensuring process efficiency: time before closure of critical CAPA (<1month); time before closure of minor CAPA (<4months); % of internal non-conformity (NC) treated in less than 1 week (>80%); % of derogation out of NC opened (<5%).
- For ensuring the process is safe: % of PMS made according to the targeted date – every year (100%); number of recalls implemented every year (≤2).

## Supplier control

Manufacturers must select and classify suppliers (e.g., critical, major, minor) based on the risk of the service and/or products provided according to the selection criteria determined by the company (e.g., impact of the supplier activity on the device safety) and the evidence provided (e.g., certification, audit results, product provided, etc.). Each supplier is then evaluated at a suitable frequency according to defined acceptance criteria (e.g., number of NC, delay). The resulting evaluation score will help determine actions necessary to increase supplier performance. The table below summarizes a process of evaluation with a risk-based approach:

**Table 3: Example of supplier management table**

| Supplier criticity | Criteria of evaluation | Score formula | | Supplier evaluation | Action |
|---|---|---|---|---|---|
| A – critical | Number of NC (A) | (Number of order with NC / number of order) *20 | (2A+B+2C)/5 | Green (≥16.00/20) | None |
| | Number of delay above 2 days (B) | (Number of order with delay (>2d) / number of order) *20 | | Orange (10.00-15.00/20) | Audit onsite |
| | Technical support (C) | (Number of technical support response within 2d / number of technical support requested) *20 | | Red (<10.00/20) | Removal of supplier |
| B – major | Number of NC (A) | (Number of order with NC / number of order) *20 | (2A+B+C)/4 | Green (≥16.00/20) | None |
| | Number of delay above 2 days (B) | (Number of order with delay (>2d) / number of order) *20 | | Orange (10.00-15.00/20) | Audit onsite |
| | Technical support (C) | (Number of technical support response within 2d / number of technical support requested) *20 | | Red (<10.00/20) | Action plan – removal after 3 recurrences |
| C - minor | Number of NC (A) | (Number of order with NC / number of order) *20 | (A+2B+2C)/5 | Green (≥16.00/20) | None |
| | Number of delay above 2 days (B) | (Number of order with delay (2d) / number of order) *20 | | Orange (10.00-15.00/20) | Action plan |
| | Technical support (C) | (Number of technical support response within 2d / number of technical support requested) *20 | | Red (<10.00/20) | Action plan after 5 recurrences |

***Source**: Emergo*

## Software validation

To include a risk-based approach in a software validation process, an organization may define acceptance criteria based on this concept to classify software, and this classification will determine the validation effort and amount of evidence necessary. Regarding the IEC 62304 standard that defines how to validate software, the US FDA has published several guidances that may help define classification and acceptance criteria, as well as associated efforts:

- General Principles of Software Validation, issued in 2002
- Guidance for the Content of Premarket Submissions for Software Contained in Medical Devices, issued in 2005
- Deciding When to Submit a 510(k) for a Software Change to an Existing Device

## Human resources

Next, a company's training procedure must integrate a risk-based approach to determine the amplitude of the training effectiveness evaluation. A method of training classification shall be established with the necessary associated effectiveness evaluation. For instance, training may be classified as:

**Table 4: Example of training effectiveness evaluation**

| Risks | Training types | Effectiveness evaluation |
|---|---|---|
| 1 | Training for qualifications (e.g., new standard, new regulation, manufacturing process, use of equipment/machine, new employee, internal auditor). | • Theoric evaluation (≥7/10; or issuance of certificate)<br>• Tutor assessment (≥7/10), if applicable<br>• Implementation (1 positive result) |
| 2 | Training following a significant QMS document update (e.g., procedure, instruction) update: change the organization practices. | • Theoric evaluation (≥7/10)<br>• Checking the absence of NC occurrence/recurrence related to the QMS document for the past two months after the training |
| 3 | Training following a non-significant QMS document update (e.g., warning, precautions…): does not change the organization practices. | • Checking the absence of NC occurrence/recurrence related to the QMS document updates for the past month after the training<br>AND/OR<br>• Questionnary (≥7/10) focused on the updates |
| 4 | Informational training (e.g., regular reminders, annual meeting to present next goals). | • None |

***Source**: Emergo*

## Product realization

The organization should define and implement a procedure to control a medical device's risks throughout its lifecycle in compliance with ISO 14971:2007 and EN ISO 14971:2012 in Europe. Moreover, all design changes must now be evaluated for their significance in regard to function, performance, usability, safety, and applicable regulatory requirements. The organization shall review and update (as applicable) its design/change form accordingly, and evaluate the impact of the change as compared to the previous criteria.

## Incoming inspections

The organization must consider the requirements of incoming QMS inspections in proportion to the risk associated with the incoming products (e.g., purchased components, materials, or finished devices) and the results of supplier evaluation. The first part may be addressed through the risk management process in compliance with ISO 14971, as the risk mitigation plan implemented should proportionally correspond to the risks associated with the purchased product.

However, the incoming inspection must now also be proportional to the results of supplier evaluations. In consequence, the organization may choose to include in each incoming inspection form (and work instructions, if applicable) a section with the requirements of reinforced control when the supplier score is not appropriate. This reinforced control may fall under various activities such as additional tests, increase of sampling plan, etc.

## Measuring equipment

As discussed in the section on Software Validation, the organization may define acceptance criteria to classify software used as part of measuring devices, which will determine the necessary validation effort. The risk-based approach must be defined based on the impact on the final device if the measurement obtained is incorrect. The previously mentioned US FDA Software guidances provide useful resources for software validation and revalidation.

## Monitoring and measurement

As part of a manufacturer's post market surveillance (PMS) process, the firm should analyze and discuss activities such as the following for each range of devices it produces:

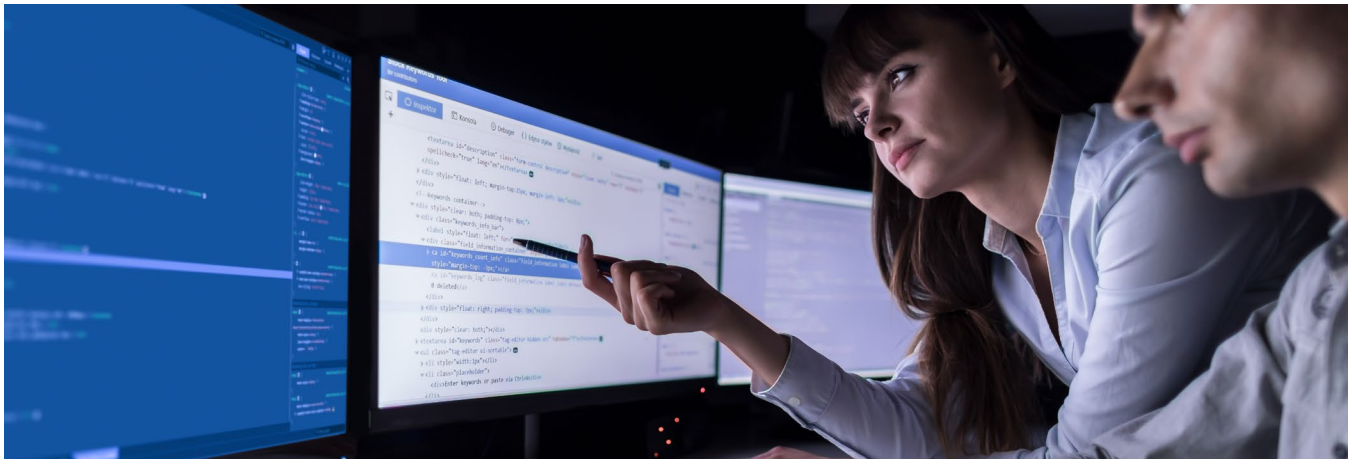
- Nonconformities
- Audits
- Complaint handling
- Vigilance
- Field safety and corrective actions (FSCA)
- Client feedback
- Change control
- Regulatory surveillance
- Clinical data review

The results of the PMS analysis must serve as input for the risk management process. In practice, the PMS report may be analyzed to:

- Detect the new risks that were not previously identified in the risk analysis.
- Review the estimation of risks (i.e., likelihood and gravity) according to the trend analyzed.

For instance, review the trend of drilling guide tip breakage and adjust the previously estimated likelihood in the risk analysis to be more accurate.

*Note: the change may lead to conducting additional risk control activities according to the new risk evaluation.*



## Internal Audits

ISO 13485:2016 requires a manufacturer to establish a QMS audit program that takes into account three factors: the process status; its importance; and the results of previous audits. The organization must consider those three criteria to establish the frequency of audits to its QMS. The importance may be classified in two categories: processes that directly affect the device (e.g., production, design control, purchasing); and processes that indirectly affect the device (e.g., training, CAPA). Then, audit frequency may be increased if the results of the previous audits and/or the status of the process (see section "Control of appropriate processes / outsourced processes") are inadequate. An example table of audit frequency:

**Table 5: Example of audit frequency evaluation**

| Importance | Process | Status | Frequency of audit |
|---|---|---|---|
| 1 – direct impact | Design Control | Appropriate | once a year |
| | | Either process status OR results of previous audit is not appropriate | every 6 months |
| | | Process status AND results of previous audit are not appropriate | every 3 months |
| 2 – indirect impact | Training | Appropriate | once a year |
| | | Either process status OR results of previous audit is not appropriate | every 9 months |
| | | Process status AND results of previous audit are not appropriate | every 6 months |

***Source**: Emergo*

## Field Safety Action

When a regulator deems a registered device nonconformant, the manufacturer must develop an action plan based on a risk evaluation. The firm may address this requirement through a process consisting of a complete investigation to determine the potential effect (i.e., severity and likelihood) of a nonconforming product detected after delivery, and especially for a field safety issue. The results will lead to different amplitudes of field safety actions. Examples of acceptance criteria and resulting field actions include:

**Table 6: Example of field safety action evaluation**
**Evaluation of effect of noncomforming device detected after delivery**

| | |
|---|---|
| Does the delivered device meet the regulatory requirements? | Yes: Recall |
| | No: Go to risk score evaluation |
| **Risk score (likelihood x severity)** | **Resulting actions** |
| 0-20 – low | None |
| 21-40 – moderate | Field safety notice |
| 41-80 - high | Recall |

***Source**: Emergo*

## CAPA

Any corrective or preventive actions (CAPA) stemming from a nonconformity must be proportional to the effect of the nonconformity encountered. Therefore, each CAPA should be classified based on the nonconformity observed. The nonconformity may be directly classified when reported (e.g., principle used in the Medical Device Single Audit Program (MDSAP)), or when a CAPA is being issued. Considering this second scenario, the CAPA may include several categories (e.g., critical/major/minor) that should define the prioritization and amplitude of corrective actions.

## Conclusions and next steps

The QMS updates in regard to ISO 13485:2016 and especially for the risk-based approach will lead to a significant change in manufacturers' forms as well as associated procedures or work instructions. Moreover, day-to-day practices will change for much of the organization's employees, making the training of ISO 13485:2016 a critical part of the implementation.

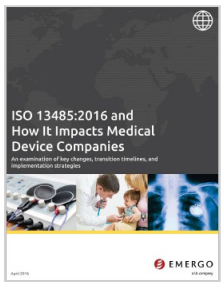
Fortunately, ISO 13485:2016 requires no retrospective review of QMS documents and records. Once the organization decides to implement the changes necessary for compliance to ISO 13485:2016, only the new records will have to conform to the new processes and procedures. However, for new risk-based requirements, new expectations from Notified Bodies or registrars auditing to the new standard, or instances where weaknesses already existed in regard to ISO 13485 compliance, the new standard could have a significant impact on the organization's activities. For instance, the validation of software, an increase in supplier control (e.g., audit), a review of incoming inspection forms, or a review of relationships between processes for consistency in terms of risk could prove time-consuming.

Though the risk-based approach is one of the new ISO 13485 standard's main changes, organizations must also consider numerous updates as well as the overall training to the standard and to the updated procedures. There are reports that some Notified Bodies will stop providing audits against ISO 13485:2003/EN ISO 13485:2012 in early 2018, and thus manufacturers may have to comply with the new revision at their 2018 audit. It is now highly recommended that organizations review the timing of their transitions with their Notified Bodies and/or ISO Registrars.

## About the Author

**Alexandre Pétiard** is a Senior Quality & Regulatory Consultant at Emergo. With more than eight years of experience in regulatory affairs, his expertise includes design control support, technical file preparation, clinical evaluation report, risk management file, 510(k), quality system implementation and audits, and post-market surveillance and vigilance activities. Mr. Pétiard previously held regulatory positions at Covidien, Integra LifeSciences, and Alcis.

# Learn More...




## Learn more about ISO 13485:2016

If you are transitioning to the new standard, this white paper outlining the major QMS changes introduced in ISO 13485:2016 will be useful. We discuss specific changes, how to prepare for the new standard, recertification requirements and deadlines, and much more.

DOWNLOAD PDF

## Need help with global regulatory compliance?

Emergo helps medical device companies with regulatory compliance and commercialization in markets worldwide.

- Medical device classification
- ISO 14971 risk management consulting
- Post-market surveillance and vigilance

LEARN MORE