

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12



13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25

**PROPOSED DRAFT SG3/N15R6**

**RISK MANAGEMENT AS AN INTEGRAL PART OF THE QUALITY MANAGEMENT SYSTEM**

25	<b><u>RISK MANAGEMENT AS AN INTEGRAL PART OF THE QUALITY MANAGEMENT SYSTEM</u></b>
26	
27	1. Introduction
28	A Purpose
29	B Scope
30	
31	2. Definitions
32	
33	3. General
34	A Documentation
35	B Communication
36	
37	4. Management Responsibilities
38	
39	5. Design and Development
40	
41	A Design and development planning
42	B Design and development input
43	C Design and development output
44	D Design and development review
45	E Design and development verification
46	F Design and development validation
47	G Control of design and development changes
48	H Design and development transfer
49	
50	6. Product Traceability
51	
52	7. Purchasing Controls and Acceptance Activities
53	
54	8. Production and Process Controls
55	A Manufacturing, Measuring and Monitoring Equipment
56	B Work Environment
57	C Personnel
58	D Process Validation
59	
60	9. Servicing
61	
62	10. CAPA
63	A Post Production Information (Post Market Surveillance, Post Marketing Studies, Servicing, Service records, Complaints, etc.)
64	B Manufacturing non-conformities/defects, Engineering Non-conformities/defects
65	C Quality System/Internal audit findings
66	
67	
68	11. Statistical Technique
69	A Valid Statistical Rationale Commensurate with Risk
70	B Data Integrity
71	C Model Validity
72	D Risk Based Interpretation
73	E Appropriate Use of Statistical Software
74	

74 Title: Risk management as an integral part of the Quality Management System

75

76 1. **Introduction:**

77

78

79 “Risk management as an integral part of the Quality Management System” is intended to  
80 assist medical device manufacturers with the integration of risk management concepts into  
81 their quality management system by providing practical explanations and examples. It is  
82 based on general principles of a quality management system and general principles of a risk  
83 management system and not on any particular standard or regulatory requirement. This  
84 document has general applicability to quality management systems for organizations  
85 providing medical devices. This document will discuss risks related to product safety, rather  
86 than other business risks. The integration of risk management into the quality management  
87 system is applicable to all stages of the life cycle of a medical device. This guidance does not  
88 suggest particular methods of implementation and therefore should not be used to assess or  
89 audit compliance with regulatory requirements.

90

91 Every medical device manufacturer has a set of management practices and processes, which  
92 together are intended to satisfy the organization’s objectives. Some of those objectives  
93 include ensuring the safety and quality of products, achieving a specified level of business  
94 performance, etc.

95

96 From a regulatory perspective, a quality management system has long been recognized as  
97 being essential for ensuring the safety and effectiveness of medical devices. Similarly, there  
98 are widely accepted principles of risk management that have been recognized as essential to  
99 medical device safety. The elements of risk management fit well into several of the quality  
100 system elements, and the discipline entailed in quality systems ensures that the reviews  
101 required in risk management are accomplished. There is a significant benefit to be derived by  
102 integrating those practices and processes that are applicable to the organization’s needs into a  
103 combined management system, rather than maintaining two separate systems that overlap and  
104 interact with one another. This guidance document describes how risk management concepts  
105 can be an integral part of a quality management system.

106

107 The integration of risk management into the quality management system is applicable to all  
108 stages of the life cycle of a medical device. A typical risk management system will consist of  
109 the following elements:

110  
111

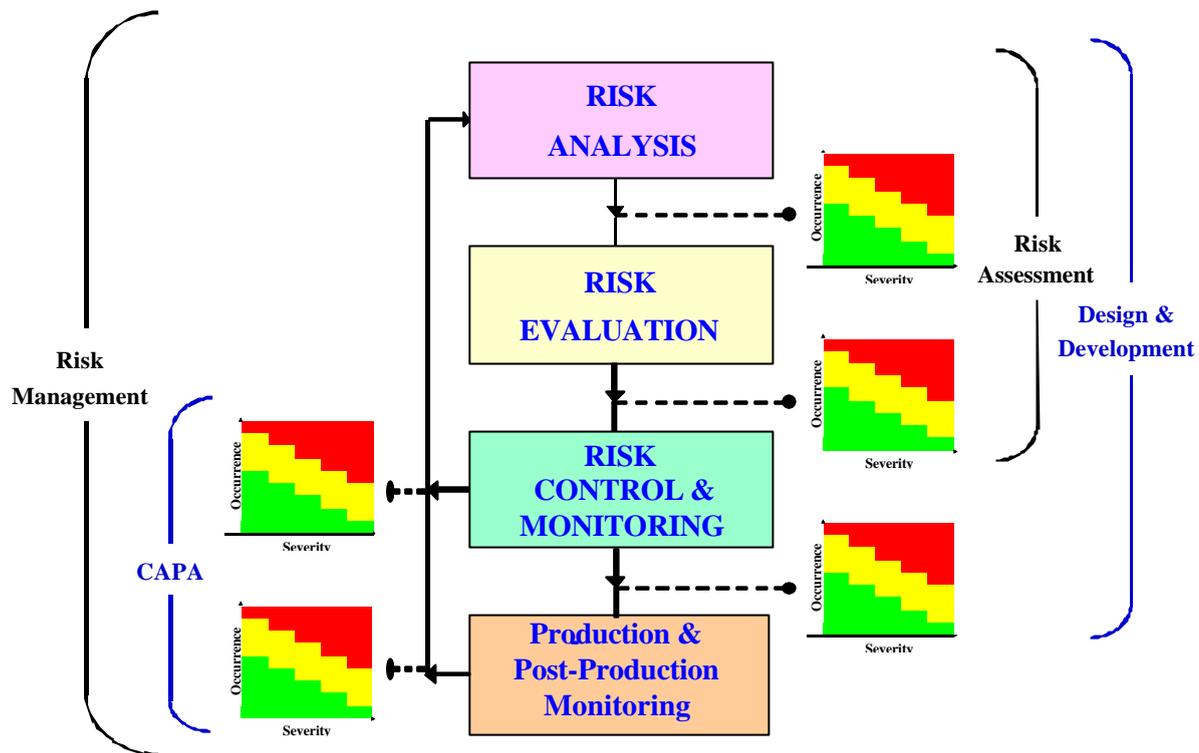


Figure 1: Risk Management System

112  
113  
114  
115  
116  
117  
118  
119  
120

Risk analysis should consist of hazard identification and estimation of the risks for the consequences of each hazard. Risk evaluation should address the acceptability of risks that have been evaluated. Risk control is the process through which decisions are reached and protective measures implemented to reduce or eliminate unacceptable risks. Monitoring of production and postproduction information provides the basis for establishing new design safety requirements as well as a baseline for future risk management of similar devices.

**A Purpose**

121  
122  
123  
124  
125  
126  
127

This guidance document is intended to assist medical device manufacturers with the integration of risk management concepts into their quality management system by providing practical explanations and examples. This guidance does not suggest particular methods of implementation and therefore must not be used to assess or audit compliance with regulatory requirements.

**B Scope**

130  
131  
132  
133  
134  
135

This document has general applicability to quality management systems for organizations providing medical devices. This document will discuss risks related to product safety, rather than other business risks. The integration of risk management into the quality management system is applicable to all stages of the life cycle of a medical device.

**2. Definitions:**

136  
137  
138

139 Definitions from ISO 14971:2000 are applicable for use in this guidance document.  
140  
141

### 142 **3. General**

#### 143 **A Documentation**

145 Requirements for risk management should be established and documented by the  
146 organization and resulting records maintained or referenced in the risk management file or  
147 other appropriate files (e.g., Design History File, Technical File/Technical Documentation,  
148 Design Dossier, Device Master Record, Device History Record, Process Validation files,  
149 etc.). The controls applied to quality management documentation should also be applied to  
150 risk management documentation.

152 While not specifically required by regulation, the risk management file, containing records  
153 and other documents associated with or resulting from risk management activity is required  
154 by certain standards. The risk management file may actually contain such records and  
155 documents or may contain references as to where such documentation may be found within  
156 the quality management system.

158 Where statutory and regulatory requirements related to risk management exist, those  
159 requirements must be observed and included in the documented procedures.

161 Certain standards require that the risk management process be documented.  
162  
163

## 163 B Communication

164

165 The communication of risk is an important ongoing activity in ensuring an effective risk  
 166 management process through out the entire product life cycle. In order to have a cohesive risk  
 167 communication process, the understanding and interpretation of risk must be consistent in the  
 168 entire organization. Certain standards provide a simple and useful risk definition. It could be  
 169 presented in a simple two-dimensional risk chart (see figure 2). Such risk charts could be  
 170 used as a communication tool through out the entire product life cycle.

171

172

Figure 2. Example of a Risk Chart (For illustration only)

Occurrence	O-6					
	O-5				HIGH	
	O-4					
	O-3			MEDIUM		
	O-2		LOW			
	O-1					
	O-0					
			S-1	S-2	S-3	S-4
Severity						

173 Another useful alignment in risk communication is the terminology used for hazards and/or  
 174 patient (human) harms. It is very beneficial for a project team to begin with a common list of  
 175 terminology on hazards and/or patient (human) harms. A project team could then continue to  
 176 conduct the risk management activities with clarity.

177

178

179

### 180 4. Management Responsibilities:

181

182 Integration of risk management into a quality management system should begin with top  
 183 management.

184

185 Top management has responsibility for demonstrating commitment by establishing quality  
 186 objectives, including those relating to product safety, and providing sufficient resources for  
 187 the implementation of an effective quality management system.

188

189 Risk management is one of those activities within product realization intended to ensure the  
 190 safety of medical devices.

191

192 It is possible to integrate the risk management activities into the quality management system.

193

194

### 195 Quality Planning

196 As part of the quality planning, management should:

197

- 198 ➤ state the approach(es) to be used in determining acceptable levels of
- 199 ➤ identify those functions having responsibility for risk management activities
- 200 ➤ identify methods to be used for review of risk management results at defined
- 201 intervals and provide input to the quality management review process.

202

203

## 203 5. Design and Development

204

205 A requirement of a quality management system is that risk management should be applied  
206 throughout product realization. This spans the whole life cycle of a product, from planning of  
207 product realization, customer-related processes, design and development, purchasing and  
208 production to service provisions and goes to the end of product life.

209

210 Design and development of a medical device is an evolutionary process, embracing many  
211 engineering and management practices. Integral to activities associated with this process are  
212 the identification and mitigation of hazards and safety concerns. The objective of risk  
213 management is rarely to eliminate all risk, but rather to reduce risk to an acceptable level.

214

215 Risk management activities should begin as early as possible in the design and development  
216 phase, when it is easier to prevent problems versus correcting them later. Risk management  
217 activities continue to the end of product life. Relying exclusively on design and development  
218 processes to control risk is not sufficient risk management. Even the best design and  
219 development processes fall short of ensuring error free design output.

220 After release of the device to market, risk management activities may be linked to quality  
221 management procedures for production and process control, corrective and preventive  
222 actions, and document control.

223

224 Certain standards require a risk management plan. The development of this plan should be  
225 incorporated into the product realization planning. Product realization planning should  
226 identify those persons or organizational functions having responsibility for risk management  
227 reviews and approvals, and include processes for review and approval.

228

229

### 230 A Design and development planning

231

232 Risk management conducted during design and development should involve different fields  
233 of expertise to ensure sufficient coverage of all concerns. A risk management process is  
234 necessary to ensure coordination of these efforts and closure of all identified issues. Design  
235 and development planning should include the risk management tasks, identify the needed  
236 resources, define the interrelationship between tasks, and define roles and responsibilities for  
237 each task.

238

239 Design and development activities targeted at mitigating risks should be supported by  
240 documentation that relates the design activity to identified risk in a way that provides  
241 objective evidence that the nature and extent of the design control is reasonable and  
242 appropriate, considering the degree of risk.

243

### 244 B Design and development input

245

246 During this phase, the requirements for a device are captured in one or more documents  
247 intended to be the foundation for subsequent design and development activities,  
248 implementation, verification, and validation. It is imperative, that the output of the risk  
249 assessment process, especially the need for control measures, should become part of the  
250 design input documentation defining the requirements necessary to ensure the safety of a  
251 device.

252

253 Risk analysis starts with the product's intended use/intended purpose and its characteristics to  
254 define the scope of the risk management activities. Other inputs are e.g. essential  
255 requirements for safety (for inherent safety design), risk related data from post-production  
256 information of products with similar design, and risk related to the manufacturing methods to  
257 be used in the production of the device. This normally results in a preliminary hazards list.  
258

259 Following the identification of known and foreseeable hazards, for each hazard the risk in  
260 both normal and fault conditions must be estimated. In the risk evaluation the manufacturer  
261 must decide whether the estimated risk is so low that risk reduction need not be pursued. If  
262 the risk is not acceptable, the need for risk control measures become part of the design input.  
263 Risk control measures are part of the design output and are evaluated to determine the  
264 residual risk. This design input/output cycle will iterate and continue throughout the overall  
265 design control process until the residual risks have been reduced to an acceptable level and  
266 can be maintained at an acceptable level.  
267

268 The need for risk control measures and other safety requirements can be compiled into a  
269 specific safety requirements document or can be integrated with other design input  
270 requirement documents. If the latter approach is taken, the requirements should be clearly  
271 identifiable as safety requirements.  
272

273  
274  
275



CHART rev2.doc  
(77 KB)

276  
277

277 **C Design and development outputs**

278

279 Design and development outputs are of three types. The Quality management system requires  
 280 specification of the characteristics of the product, including those essential for its safe and  
 281 proper use. Design outputs relating to purchasing, production, and service processes, and  
 282 acceptance criteria may also be essential for safe and proper use. Risk control measures may  
 283 fall into any of these categories. The following table shows examples of each type of risk  
 284 control measure.

285

Design and development output type	Examples of risk control measures
Product characteristics	<ul style="list-style-type: none"> <li>• Compliance with IEC 60601</li> <li>• Over-temperature alarm</li> <li>• Warning label on device</li> <li>• User training</li> <li>• Redundant power source on a life-support device</li> <li>• Interlock switch on access door of an x-ray cabinet</li> <li>• Watchdog timer (in a microprocessor-based device)</li> </ul>
information related to purchasing, production and service provisions	<ul style="list-style-type: none"> <li>• special quality requirements in contracts</li> <li>• imposing stringent process controls</li> <li>• mandatory part replacements in planned maintenance service intervals for process equipment or the medical device itself</li> <li>• limitation of lot sizes</li> <li>• storage requirements</li> </ul>
product acceptance criteria	<ul style="list-style-type: none"> <li>• Torque specification for a threaded fastener</li> <li>• Dimensional tolerances for a vacuum line fitting</li> <li>• Sterility requirements for a device or accessory</li> <li>• Electrical safety performance limits (e.g., leakage current, insulation strength)</li> </ul>

286

287 One of the design outputs will be the risk control measures and where those risk control  
 288 measures will be applied.

289

290 When the design and development process for inherent safety and/or design for protective  
 291 measures are not practicable, additional risk control measures may be necessary design  
 292 outputs. These risk control measures should also have a total life cycle focus. The focus may  
 293 begin with risk control planning from the supplying of raw materials to the manufacturing of  
 294 products, from storage and distribution of the product to the use of products, from the use of  
 295 products to the patients, from the disposal of products to the next generation of products, etc.  
 296 Risk control information should be understood, identified and analyzed by the design and  
 297 development team.

298

299

300

## 300 **D Design and development review**

301

302 Top management has ultimate responsibility to ensure the safety and performance of the  
303 product, therefore, the organization must determine if the overall risk to patients, users and  
304 other persons is acceptable.

305 Design and development reviews should include review of the risk assessment (risk analysis  
306 and risk evaluation) results. Reviewers should have the necessary breadth and depth of  
307 experience to assess design decisions concerning risk acceptability.

308

309 Design review procedures should define risk review tasks that should be performed at  
310 appropriate stages of design and development. For example:

311 • At early design and development reviews, the focus will be on hazard  
312 identification, risk estimation, and the needs/requirements for risk control  
313 measures

314 • At later stages of design and development the review focus should shift to the  
315 implementation of risk control measures and evaluation of residual risk. As  
316 one progresses through verification and validation, the effectiveness of risk  
317 control measures need to be reviewed.

318 • The final design review includes overall residual risk evaluation after  
319 completing the evaluation of all single identified hazards. As a last step, if the  
320 residual risk is still too high for acceptance, a risk/benefit analysis can be  
321 performed to determine if the medical benefits outweigh the remaining risks.

322

## 323 **E Design and development verification**

324

325 Verification procedures should define appropriate analytical techniques and test methods  
326 related to safety requirements.

327 Verification procedures should ensure the results are traceable between identified hazards,  
328 causes, risk control measures, product design and development requirements, tests and test  
329 results. For an example see Annex A1.

330

## 331 **F Design and development validation**

332

333 Validation confirms the product meets user needs, intended uses, and the effectiveness of  
334 certain risk control measures. It is not necessarily a single isolated activity but may consist of  
335 a series or a culmination of activities throughout the product realization process.

336

337 From a risk management perspective, validation should confirm assumptions made about  
338 safety and the effectiveness of risk control measures. In addition, unforeseen hazards which  
339 could exist at user sites and facilities (e.g. environmental conditions like high humidity and/or  
340 extreme temperatures, unstable power supply, insufficient hygienic conditions) that emerge  
341 from validation need to be assessed and, if necessary, mitigated.

342

## 343 **G Control of design and development changes**

344

345 History has repeatedly demonstrated that seemingly trivial changes may have unforeseen and  
346 sometimes catastrophic consequences.

347

348 Proposed changes to the product and product realization processes should be evaluated for  
349 their effect(s) on the safety of the product. This evaluation should be based on criteria for risk  
350 acceptability contained in risk management and product realization records and documents.

351  
352  
353  
354  
355  
356  
357  
358  
359  
360  
361  
362  
363  
364  
365  
366  
367  
368  
369  
370  
371  
372  
373  
374  
375  
376  
377  
378  
379  
380  
381  
382  
383  
384  
385  
386  
387  
388  
389  
390  
391  
392  
393  
394  
395  
396  
397  
398  
399  
400  
401

Changes can occur at any time in the life cycle of the product. Some of these changes can introduce new hazards, eliminate existing hazards, or change the level of risk associated with a hazard. A change could be the result of a risk reduction measure or a re-evaluation of the original risk assessment. Therefore, if a change takes place after a risk assessment has been completed, the risk assessment should be reviewed and updated as necessary.

In the risk assessment of a change, consider that a change of material (even nominally identical material from a different supplier) may have an impact on the safety of a device (for example, biological or physical). Similarly, replacement of one machine in a process by another may have unforeseen consequences. Seemingly trivial changes to a process may have cumulative effects which may lead to a requirement for a process revalidation. If a medical device can be reused, the effect of any reprocessing should be evaluated on the device after the change. Changes to the sterilization of a medical device should also be considered very carefully.

Prior to implementing a proposed change, it is important to ensure that any residual risk(s) are defined and remain acceptable.

If circumstances arise under which established acceptability criteria need to be changed, this needs to be documented along with the rationale and evidence supporting this decision.

## **H Design and development transfer**

The transfer of a new or changed design to production is a key transition in the life cycle of a medical device. For many medical devices, the design transfer is not a single event, but a complex series of staged transitions as the design evolves from the prototype stage through production process validation activities, clinical trials, and finally release to market. The design transfer is even more challenging when outsourced or off-shore operations are involved in the manufacture or servicing of the device. In some cases, intensive design and development activities continue past initial release to market as the design and production processes are further optimized based on evolving market demands, business needs, and/or experience gained with the product.

Design and development plans should define those design transfer activities that are required to assure the adequacy of production specifications at each such life cycle transition. Design transfer procedures generally involve some combination of verification, validation, review, and documented approvals. The exact mix of these elements should be reasonably appropriate, considering the technologies involved and factors mentioned above.

One key aspect of product quality that must be addressed in each case is product safety. Thus, risk management plays an important role in design transfer. In general, the design transfer procedure should ensure that safety issues are resolved to the satisfaction of all interested parties prior to the release of the device to production and/or market. However, there are few absolutes in making such a determination. For example, a clinical evaluation, using production devices, may be needed to characterize or validate some aspect of medical device risk. Thus, the release to production for the purpose of conducting the clinical evaluation is necessary to complete the risk evaluation. On the other hand, it would be unethical and inappropriate to conduct the clinical evaluation until those aspects of device risk that can be evaluated with reasonable certainty have been addressed.

402 As the production specifications approach finality (realizing that few things in the life cycle  
403 of a medical device are ever really “final”), the risk evaluation must be increasingly  
404 comprehensive. In most cases, this requires not only reasonable assurance that all  
405 foreseeable risks have been addressed, but some sort of documentation of the overall  
406 acceptability of any and all residual risk associated with the product. This inevitably is a  
407 subjective judgment made by senior management. The decision should be based on the  
408 documented risk acceptability criteria as described previously in this guidance. The design  
409 transfer procedure should identify those persons or functions responsible for making risk  
410 acceptability decisions and provide mechanisms for documenting such approvals. The  
411 procedure may also require a documented rationale when the basis of the decision is not  
412 apparent from the record.

413

414

415

## 415 **6. Product Traceability:**

### 416 **Traceability**

417 Under a quality management system, a manufacturer should establish documented procedures  
418 for traceability based on the risk. The procedures should define the extent of traceability and  
419 which components and which products should be followed.

420 Product traceability involves the ability to trace the history and also facilitate the control of  
421 non-conforming product. Traceability is typically required when there is a need to track a  
422 nonconformity back to its source for investigation as part of CAPA implementation.

423  
424 Product traceability can determine the location of the remainder of an affected batch and can  
425 help with the issuance of advisory notices and recalls.

426  
427 Sometimes the extent of traceability can be a requirement of a regulatory authority. But in  
428 many cases, risk assessment will help the manufacturer to define the proper extent of  
429 traceability.

430  
431 Traceability need not be applied to every product. Several points need to be considered, such  
432 as:

- 433
- 434 ➤ The risk associated with a device: life sustaining or implantable
  - 435 ➤ The probability of failure
  - 436 ➤ The consequence of the failure: led to the death of a patient, or user or of other  
437 persons or to a serious deterioration in their state of health;
- 438

439 The extent of traceability should be defined regarding the following activities: receiving,  
440 production, warehousing, distribution, installation, servicing processes, up to the point when  
441 the product leaves the organization's possession. Even identification of samples during  
442 laboratory testing may need to be evaluated.

443  
444 During the receiving activities, risk analysis should be conducted to define what components  
445 and or materials will impact the specifications and safety of the product. These components  
446 may need traceability. The manufacturer should have procedures in place describing the  
447 application of the risk analysis process is applied to receiving activities and the criteria for  
448 deciding when traceability should be applied to an incoming goods or service.

449  
450 Relating to the intermediate products and finished products, risk analysis should be  
451 conducted to define the critical points of the process. If any process controls are necessary to  
452 ensure conformance to specifications, the necessity to implement traceability after each  
453 validated critical point should be studied.

454  
455 Risk analysis should define the equipment and/or the environmental conditions when this  
456 could cause the medical device not to satisfy its specified requirement. In each case  
457 traceability should be studied

458  
459 After the decision to implement traceability in a step, the level of the detail should be  
460 evaluated from simple unit to batch.

### 461 462 **Product identification/Traceability:**

463

464 During the risk management activities, the organization shall take appropriate measures to  
465 identify the products at each step, following documented procedure.

466

467 For each identified products, the organization should documented the appropriate meanings  
468 by which the following items are identified:

469

470 - characteristics related to the safety of the product

471 - known or foreseeable hazards associated with a medical devices

472 - risk control measures

473 - new hazards introduced by risk control measures

474

475 Consequently, the organization should demonstrate that each identify hazards have been  
476 address by the risk management process and by what means (risk control measures,  
477 residual risk acceptability, etc...).

478

479 During the risk management process, Identification of personnel responsibility for execution  
480 shall be recorded for appropriate/critical responsibility (e.g. reviewer, expert, verification,  
481 approval authority)

482

## 483 **7. Controls and Acceptance:**

484

### 485 **Purchasing and Acceptance Activities**

486 Risk to the patient and consumer can be introduced into the product anywhere during the  
487 product life cycle, including outsourced product and services used during product realization.

488 The manufacturer is responsible for fully understanding the residual risks associated with the  
489 product or service procured. Therefore an effective risk management system includes  
490 procedures for identification of hazards and assessment of risks introduced by vendors early  
491 on in the product realization process, and clarifies the risk management roles and  
492 responsibilities of the manufacturer and supplier.

493

494 In addition, the quality management system should include documented procedures to ensure  
495 that purchased product and services conforms to specified purchase requirements. Specified  
496 purchase requirements should be determined with consideration to prescribed risk control  
497 measures derived from the risk management process during product realization.

498

499 The type and extent of control applied to the supplier and the purchased product and services  
500 should be dependent upon the effect of the purchased product and services on subsequent  
501 product realization or the final product including hazards identified during risk analysis.

502

503 Suppliers should be evaluated and selected based on their ability to supply product and  
504 services in accordance with the organization's requirements. Established criteria for  
505 selection, evaluation and re-evaluation of suppliers of purchased products and services  
506 should also be based upon the risk of identified hazards related to the purchased products and  
507 services determined during the risk management process.

508

509 The manufacturer should establish and implement the inspection or other activities necessary  
510 for ensuring that purchased product and services meets specified purchase requirements.

511 These activities should include prescribed risk control measures.

512

513 The manufacturer would likely utilize a combination of purchasing controls and acceptance  
514 activities to mitigate the risks introduced by the outsourced product or service. The specific  
515 levels of purchasing control and ratio of acceptance activities to purchasing control would be  
516 dependent upon the residual risk associated with the outsourced product or service.  
517  
518

## 518 8. **Production and Process Controls**

519

520 Manufacturers develop, conduct, control and monitor manufacturing processes to produce  
521 devices that conform to specifications. During the design and development of a particular  
522 device, hazards are identified and the sources of those hazards should be determined. One  
523 possibility is that the source(s) of the hazard are the actual manufacturing processes, which  
524 can include variability from equipment, work environment, personnel, etc. An effective  
525 quality management system includes document procedures that assess and controls these  
526 risks.

527

528 The risk controls developed as a result of the product risk assessments will lead to the  
529 development of appropriate methods for measuring and monitoring those manufacturing  
530 processes.

531

532 Sources of identified hazards can come from product, process, or user interface(s)

533

534 Assessment of the risks from manufacturing processes, using tools such as HACCP, HAZOP,  
535 Process FMEA, etc., can help establish or improve process controls by identifying:

536

- 537 ➤ what can go wrong at each step of the process,
- 538 ➤ the impact of failure on the product,
- 539 ➤ the likelihood of the failures, and
- 540 ➤ controls to detect and prevent the failure or causes.

541

542 Post production information such as complaints, the rate of nonconformities, the rate of  
543 rework, and other outputs of the corrective and preventive action system will then be utilized  
544 to determine the effectiveness of the process controls and measuring and monitoring systems.

545

### 546 A **Manufacturing, Measuring and Monitoring Equipment**

547

548 The risk assessment of manufacturing processes should evaluate the suitability of equipment  
549 for use in the manufacture of a specific device(s) and where applicable the maintenance,  
550 adjustments, cleaning, calibration and work instructions for equipment involved in the  
551 process being analyzed. The frequency of such activities like maintenance, adjustments,  
552 cleaning and calibration need to be assessed in relationship to the risk. The frequency may  
553 then need to be increased or decreased as a result of the risk assessment and applied risk  
554 reduction or risk control measures imposed on the process. In addition, the adequacy of any  
555 work instructions needs to be evaluated in relationship to the risk assessment and possible  
556 risk reduction or risk control measures decided upon for that process.

557

558

559

### 560 B **Work Environment**

561

562 As a part of the risk assessment of manufacturing processes the work environment should be  
563 assessed to determine if there are environmental conditions that exist or are reasonably  
564 foreseeable that may adversely affect the product or the controls/monitoring processes.  
565 Where environmental conditions are determined to have an adverse effect or produce an  
566 unacceptable risk, risk reduction or risk control measures should be defined, documented and  
567 implemented. The effectiveness of these environmental risk reduction or risk control  
568 measures should periodically be assessed.

569

570

**C Personnel**

571

572

573

574

575

576

577

578

579

An additional consideration that should be evaluated as a part of the risk assessment is the impact of personnel on the product, process, or work environment (e.g., health, cleanliness, personnel practices, clothing of personnel, experience, education, qualification, training, etc.). If contact between such personnel and product, process or environment could reasonably be expected to have an adverse effect on the product the risk must be mitigated and controlled. Those mitigation and control measures should be defined, documented, implemented and monitored, as well as evaluated for effectiveness.

580

**D Process Validation**

581

582

583

Process validation is a way of confirming the effectiveness of risk reduction activities for particular manufacturing processes.

584

585

586

587

Activities as a result of process validation can also be a risk control/reduction measure by establishing process parameters and controls (for example, when the source of an identified hazard is process variability).

588

589

590

591

When design or process changes occur, the manufacturer should perform an evaluation and document whether revalidation is required. This should ensure that the process will continue to produce results that meet specifications. The current risk assessment may be used to help determine the need for, or the extent of, any revalidation.

592

593

594

It is also important to ensure that a change does not lead to any additional hazards or increases risk.

595

**9. Servicing:**

596

597

**A Control of servicing activities**

598

599

600

601

“Servicing” used in this clause means, mainly repair and maintenance activities of medical devices.

602

603

604

605

606

If the safety of a medical device depends on the provision of maintenance as an output of the design and development process, then appropriate controls should be planned and applied to servicing activities. Periodic maintenance as a means to ensure safe functioning of a device can be one method of risk reduction.

607

608

609

610

611

612

613

614

615

Lack of appropriate controls of servicing activities could adversely affect the safety and/or performance of a device. As an example, a design engineer may decide, during the risk analysis, evaluation and control at the design and development stage of a medical device that a certain type of control needs to be applied to a particular production process to control a risk of the medical device. However, the design engineer may easily overlook the needs of similar control on a servicing process. It is important to know for the design engineer that if a certain control of a production process is decided to be necessary to control of a risk, same (or similar) control should be applied to a same (or similar) servicing process.

616

Therefore, comparable controls as in manufacturing should be applied to servicing activities.

617  
618  
619

## 619 **B Data analysis of servicing activities**

620

621 Manufacturers should establish and maintain a procedure for systematic review of  
622 information gained from the servicing activities of the medical devices or similar devices in  
623 the post-production phase. This information should be evaluated for possible impact on the  
624 current risk analysis and control measures.

625

626 If the previous analysis was invalidated or the risk controls are inadequate, this information  
627 should be fed back as input to the risk management process (see also CAPA of this  
628 guidance).

629

### 630 **10. CAPA:**

631

632 Risk management is an integral part of the quality management system CAPA  
633 processes. It provides the mechanism for determining the severity of items identified in  
634 one's specific quality data points (such as complaints, service reports, manufacturing  
635 defects, engineering non-conformities, supplier audits, and external/internal audits).

636 The CAPA process combined with risk management output facilitates a closed loop  
637 process and may be a measure of the quality system effectiveness. An effective risk  
638 based CAPA system will utilize a systematic procedure to review information gained  
639 about the device or similar devices for possible relevance to safety. For example the  
640 procedure would ensure that any previously unrecognized risks were identified,  
641 determine if the estimation of risk arising from a hazard is still acceptable; and if the  
642 original risk assessment is still valid.

643

644 For example, a service report indicating a problem with a device is reported to a  
645 manufacturer - review of the risk acceptance decision(s) confirms that a manufacturing  
646 process previously thought to have been mitigated is a contributing factor to the  
647 reported problem. An investigation into root cause and a review of the risk  
648 management process may be initiated as a result of the information from this report.  
649 Upon completion of the root cause analysis and the risk management process  
650 corrective action would be initiated.

651 This then prompts CAPA actions, such as (but not limited to):

652

653 ➤ Product Change

654 ➤ Process Change

655 ➤ Supplier Change Notice

656 ➤ Field Upgrade to installed base

657 ➤ Input for New Products

658 ➤ Input to RM process start

659 ➤ No CA, but with rationale (such as further trending, etc)

660

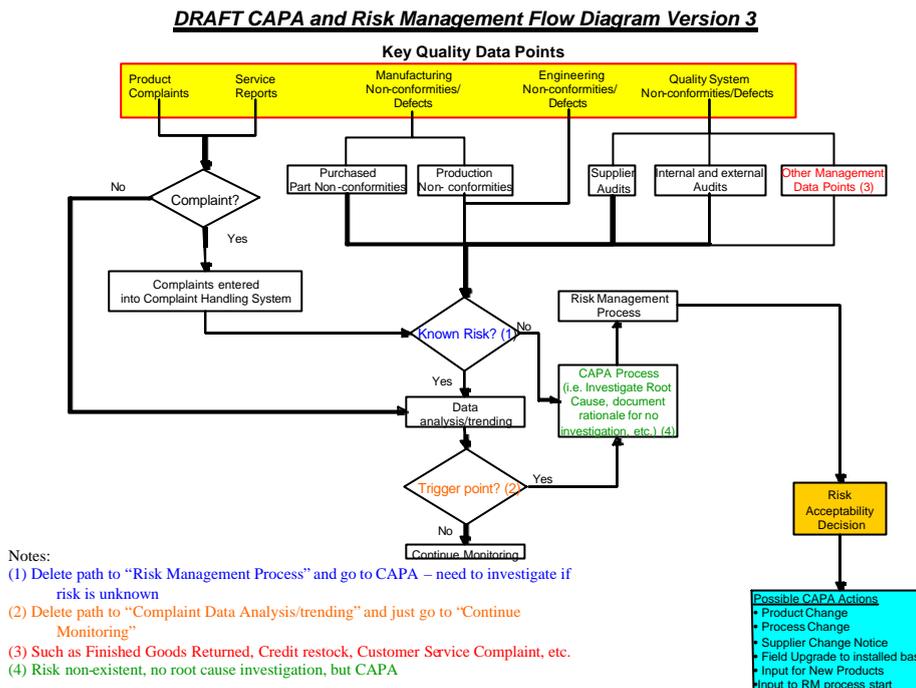


Figure 2: CAPA and Risk Management Flow Diagram

11. Statistical Techniques:

The organization should establish the proper use of risk analysis techniques including qualitative, quantitative, probabilistic and statistical analyses. When quantitative, probabilistic and statistical analyses are appropriate for risk management activities, the following principles should be applied:

**A Valid statistical rationale commensurate with risk**

Statistical and probability methods may be applied to but are not limited to: Risk Estimation, Risk Evaluation, Risk Control, Acceptability of Residual Risk, Purchasing Controls and Acceptance Activities, Product and Process Controls, Corrective and Preventive Action, and Design Changes.

**B Data integrity**

Data used for Risk Management Activities should have integrity. The purpose for collecting the data should be defined, the source of the data should be documented, valid and traceable, and the data should be sufficient, accurate and precise for the purpose.

**C Model validity**

The mathematical and/or statistical model used should fit the data (not forcing the data to the model, i.e. just plug the numbers into an equation), validity of the model and data should be checked, (all models are approximations but some are useful). Those techniques, the model (the behavior of the system, process, or products) representing the process, system or product, and the data available should be consistent with each other. The statistical method (e.g. chi-square, regression methods, estimation methods, maximum likelihood methods, etc.) should be appropriate for the mathematical model (e.g. Arrhenius Model for aging studies, Operating characteristic curves for statistical sampling plan, Reliability prediction models, such as Weibull, Exponential, etc.) used, the model should fit the data to be analyzed.

698  
699  
700  
701  
702  
703  
704  
705  
706  
707  
708  
709  
710  
711  
712  
713  
714  
715

#### **D Risk-based interpretation**

Information provided by the fitted model should provide the basis for drawing conclusions and making decisions based on risk. Only statistical and probability methods appropriate for the purpose of risk management should be employed. Examples include but are not limited to: FMEA, FTA, SPC/SQC, and Acceptance Sampling. Statistical and probability techniques employed should be appropriate for the product or process being studied.

#### **E Appropriate use of statistical software**

Statistical software tools used in risk management activities should be validated. Some commonly used software tools are valid for more sophisticated statistical analyses while others are good only for simple summary statistics such as mean, standard deviation and should not be used for more complicated analyses such as analysis of variances studies.

## 715 Annex A1 Example of Risk Management Summary Table

716

717 This example shows a fragment of a risk management summary table for a hypothetical  
 718 infusion pump. Following is a description of the structure of the table, and an example of  
 719 how the table might be used by a product development manager, internal reviewer, or  
 720 external reviewer.  
 721

HazID (A)	Contributing Factors (A)	Risk level before mitigation (B)	Risk level after mitigation (B)	Risk Control Method(s) (C)	RqtID (D)	TestID (D)	Status (E)
<b>3.0 Dosage Hazards</b>							
<b>3.1 Overdose</b>							
3.1.1	User setup error	I-B	I-D	a) Alphanumeric display shows delivery rate and units	HRD 4.5.2	STP 3.5	Pass
				b) (Barcode Option) Delivery rate encoded in prescription barcode; user prompted to scan patient bracelet and confirm settings	HRD 8.3 SRD 12.6	STP 22.1 thru 22.5	Pass
3.1.2	Tampering with settings	I-B	I-D	Keyboard lock prevents unauthorized setting change	SRD 7.2	STP 17	Awaiting test
3.1.3	Pump over-run due to microprocessor lockup	I-B	II-D	a) Blocking capacitor limits pump on time to a maximum of one second	HRD 9.2	STP 32.0	Pass
				b) Watchdog timer interrupts power to pump	HRD 10.5	STP 26.2	Pass
<b>3.2 Under-dose</b>							
.							
.							
.							

722

723

724 **A. Hazard Identification (HazID)**

725

726 In this example, risks are identified using a three-level hierarchy. (Other organizations are  
 727 possible.) The top level of the hierarchy is the major classes of hazards. For example, in an  
 728 infusion pump, some of the major classes of hazards might include:

729

- 730 1.0 Energy hazards
- 731 2.0 Mechanical hazards
- 732 3.0 Dosage hazards

733

734 The second level of hazard classification identifies particular hazards. For example, in an  
 735 infusion pump, two hazards related to dosage are:

736

- 737 3.1 Overdose
- 738 3.2 Under-dose

739

740 The third level of hazard classification is a particular cause or contributing factor. Typically,  
 741 a given hazard may have multiple causes or contributing factors, combinations of which lead  
 742 to similar outcomes, as shown in the example.

743

744 **B. Risk Evaluation**

745

746 These two columns show the results of risk evaluation before and after mitigation. In this  
 747 example, the risk level is characterized by a coding scheme using Roman numerals and letters  
 748 to denote estimates for severity and likelihood, respectively. The color or shading of the cell

749 represents the manufacturer’s grading of risk acceptability (e.g., intolerable, undesirable,  
750 tolerable, negligible). The details of the scheme used by this manufacturer are not important  
751 for this example. Other manufacturers may employ different approaches to risk evaluation,  
752 but the results in any case would be summarized in these two columns.

753

### 754 **C. Risk Control Measures**

755

756 This column describes or summarizes the risk controls measures which form the basis for the  
757 risk reduction shown. The actual risk scenarios and risk control measures might be far more  
758 complex than is possible to describe in a short summary paragraph. In that case, the entry in  
759 this column might refer the interested reader to another document which describes the risk  
760 control measures in more detail.

761

### 762 **D. Traceability Data (RqtID and TestID)**

763

764 These two columns provide traceability between control measures, product design  
765 requirements, and verification/validation activities. The column labeled “Requirement  
766 Identification” (RqtID) points to relevant clauses in the product design documentation that  
767 define requirements relating to a given risk control measure. The column labeled “Test  
768 Identification” (TestID) points to clauses in test procedures or other verification and  
769 validation documents that confirm that the control measure was adequately implemented.

770

771 In the example, “HRD” refers to the product Hardware Requirements Document, and “SRD”  
772 refers to the Software Requirements Document. “STP” refers to the System Test Procedure  
773 for this particular device.

774

### 775 **E. Status Information**

776

777 The last column is used during product development to track progress in completing risk  
778 management activities. This example uses cell color or shading to highlight incomplete  
779 activities.

780

### 781 **Example of Use of the Table**

782

783 As an example of how to use the risk management summary table, consider the entry for  
784 HazID 3.1.2. This entry describes the use of a keyboard lock to prevent unauthorized  
785 changes to device settings. This control method mitigates one possible scenario leading to  
786 patient overdose (and would presumably be listed as a mitigation method for the hazard of  
787 under-dose as well). The keyboard lock mechanism was judged to reduce risk from a level of  
788 I-B to I-D, reflecting reduced likelihood of the hazardous event. The requirement for a  
789 keyboard lock was captured in the Software Requirements Document, paragraph 7.2, and the  
790 functionality of the keyboard lock was tested in Section 17 of the System Test Procedure.  
791 The last column indicates that the results of this testing are not yet available.

792

793 Note that this summary table overlooks much of the complexity of the situation. For  
794 example, the table makes it apparent that this manufacturer chose to implement the keyboard  
795 lock function in software. There is no indication of the relative merits of implementing the  
796 function in hardware versus software. The table also lacks a detailed explanation of how the  
797 keyboard lock function works, and what new hazards this function might introduce.

798

799 However, the interested reviewer can make an independent judgment about the  
reasonableness of the manufacturer’s risk estimates, and review the referenced documents for

800 additional information. Thus, the summary table provides a reasonable basis for quickly  
801 assessing the completeness and comprehensiveness of the manufacturer's risk management  
802 activities, and identifying potential areas of concern.  
803  
804

**804 Annex A2**

805

806 For software the same requirements of the risk management process applies as for hardware.  
807 Since the risks resulting from software cannot be determined without the hardware  
808 components, the risk assessment and risk control activities have always encompass the device  
809 as a whole. Differences in the risk management for software due to its specific characteristics  
810 compared to hardware have to be considered in each step of the risk management activities.  
811 Information about risk management for software can be found in specific standards and  
812 guidelines/guidance, e.g. for software life cycle and software validation.

813

814 The risk management for software needs to be planned and performed depending on the type  
815 and integration status of the software:

816

817 a) The software is an integral component of the medical device, e.g. software which controls  
818 the functions of a device. The software related risk management activities are part of the  
819 overall risk management activities for the device.

820

821 b) The software is a medical device in its own right, e.g. a computer program, delivered on a  
822 CD-ROM and running on specified PC configurations. Although the software is basically  
823 independent from a dedicated hardware, the risk management measures have to include  
824 the possible hardware(s) necessary for its use.

825

826 c) The software is an accessory to a medical device, e.g. providing statistical evaluation  
827 functions, and runs independent from the basic medical device software. Risk  
828 management must be applied in the same way as for “b) a medical device software in its  
829 own right”, and in addition the links and the interoperability between the medical device  
830 and the accessory software need to be considered.

831

832 d) “Off the shelf” (OTS) software like operating systems, software development tools, data  
833 base software, etc., used in design and development activities or at run-time. All OTS  
834 software must be included in the risk management activities, depending on its use in the  
835 software life cycle phase.

836

837 Software combinations, consisting of multiple, interactive user/application software on a  
838 single computer processor. Such combinations can consist of medical and non-medical device  
839 software. Examples for such combinations can be found e.g. in capital imaging equipments  
840 like MRI or CT units with separate but interacting software for data acquisition, data display,  
841 data evaluation, file management and networking capabilities which offer not only access to  
842 data archives but also access to administration as well as radiology and/or laboratory  
843 information.

844

844  
845  
846  
847  
848  
849  
850  
851  
852  
853  
854  
855  
856  
857  
858  
859  
860  
861  
862

### **Bibliography**

- ISO 9000:2000** Quality management systems – Fundamentals and vocabulary
- ISO 13485:2003** Medical devices – Quality management systems – System requirements for regulatory purposes
- ISO 14971:2000** Medical devices – Application of risk management to medical devices
- IEC/1CD 62304** Medical device software - Software life cycle processes  
(developed by IEC/SC 62A and ISO/TC 210 JWG 3, date of circulation 2003-01-17, closing dates for comments 2003-04-21)
- General Principles of Software Validation;** Final Guidance for Industry and for FDA Staff  
(FDA/CDRH, issued January 11, 2002)
- Off-The-Shelf Software Use in Medical Devices;** Guidance for Industry, FDA Reviewers and Compliance on (FDA/CDRH, issued on September 9, 1999)

862  
863  
864  
865

**This Page Intentionally Left Blank**