10.I.2 General Items on the FMEA Process

A general FMEA process can be run formally in 10 steps after establishing a team. These steps are in line with the risk management process described in ICH Q9. Figure 10.I-1 shows the FMEA process flow with ten steps:

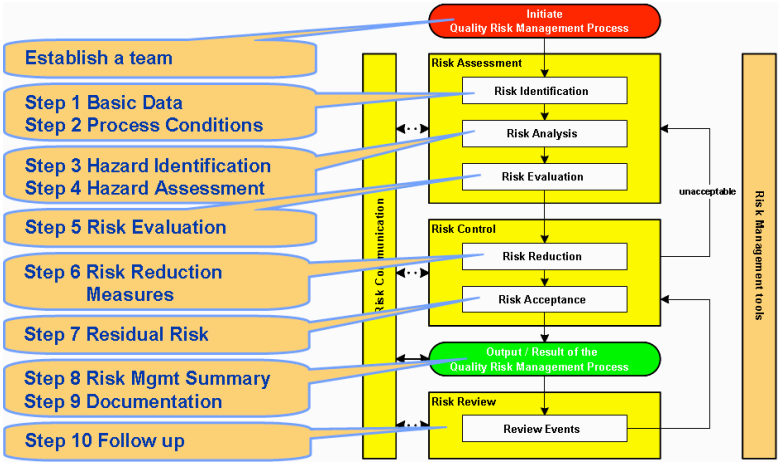

Figure 10.I-1 FMEA process flow

The preparation of the necessary process information can be done by these procedures:

1. Collect Basic data
2. Describe process conditions
3. Hazard identification e.g. identification of possible failures, consequences and cause of failure
4. Hazard assessment (Risk Analysis)
5. Evaluation of the failure and determination of the risk priority number (**RPN**)
6. Definition of reductions measures
7. Awareness of the residual risks
8. Summary of the results
9. Documentation of the performed process
10. Follow up and the implementation of measures

During the identification of potential failures, it is important not to concentrate on GMP-relevant failures only. In practice, it has shown to be more useful to include as many types of potential failure as possible (e.g. business risks, environmental risks, patient safety risks). These measures are taken in case the customer is a manufacturing facility and GMP risks are not the only ones, which influence the performance and at least the availability of the drug.

It initially means a large documentation effort, which is not necessarily required for regulatory purposes. There also are advantages: for example, the potential risks for business-critical processes in accounting should also be identified, so that if necessary, measures can also be established to minimize non-GMP risks and thus make the processes more stable and reliable. This leads to a kind of total quality management. It has been shown that the risk management tools in the different disciplines are in principle the same. Why not combine the efforts?

10.I.2.1 Step 1: Preparation of the Necessary Process Information – Collect Basic Data

For the execution of a **FMEA** and all other forms of risk assessment the scope of the assessment should be established first. Therefore, the technique of process mapping as described earlier is helpful. Initially, the respective overall process structure should be displayed and then subdivided (generally on multiple levels) into further detailed sub-processing steps. The description is mainly used to map the process to be analyzed and its interfaces. Furthermore, structuring the processes on different levels enables classification according to level of detail and possible influence exerted.

10.I.2.2 Step 2: Preparation of the Necessary Process Information – Describe Process Conditions

All relevant process information must be available e.g. examples of useful documents could be manufacturing reports or test specification.

The individual process steps e.g. mapped in a process map are assigned unique numbers to enable clear referencing at a later stage. In the example below the steps have been numbered in increments of ten so that it is subsequently possible to insert additional sub-processes (e.g. if an extra control balance is integrated into the overall process at a later stage). The figure provides an overview of a simple flow chart with three levels of detail (figure 10.I-2).

10.I.2.3 Step 3: Identification of Possible Failures, Consequences and Cause of Failure – Hazard Identification

The identification of possible failures, their consequences, and causes of failure is the most time-consuming part of the FMEA. Each individual processing step is analyzed at all levels for possible failures. All potential **influencing factors** should be taken into account (normally the **five Ms**, i.e. machinery, manpower, material, method, and milieu like environment (see section on fish bone diagram).

Failures that may seem hypothetical should also be taken into account, since the probability of occurrence is not considered until a later stage of the FMEA.

The identification of possible failures is time-consuming, particularly in the initial phase of the execution of FMEAs. It can be done by brainstorming or using an available list of potential hazards e.g. for a unit operation. When several similar

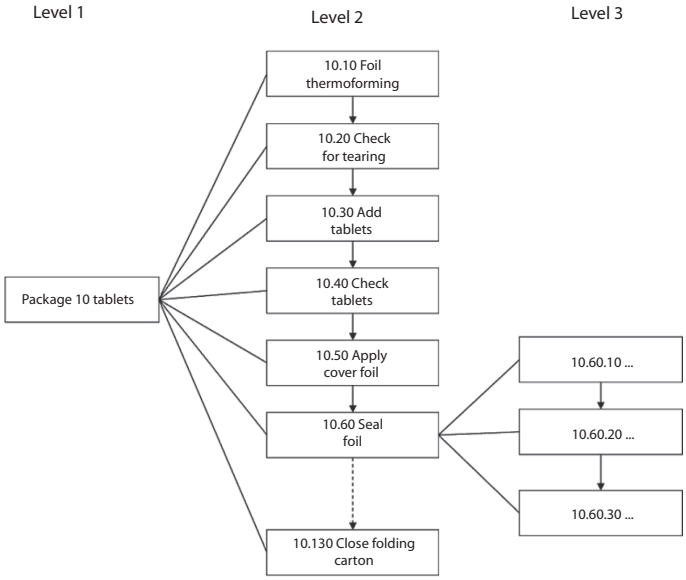

Figure 10.I-2 Example of a flow chart of a tablet packaging process

processes, systems or facilities have already been assessed, there may be similarities in the occurrence of failures, and the work required for this phase is reduced. In general, potential failures are identified by team members who actually implement the processes, systems and/or work with the facilities. The team should be compiled from interdisciplinary members (e.g. from production, laboratory, quality assurance, engineering, information processing) and from different hierarchies if necessary, but should also not consist of more than 6-8 participants to ensure that it can still function effectively. One suitable method for recording potential failures is, for example, brainstorming.

At this point of time it is important to take into account regulatory compliance. It means to consider all relevant requirements of authorities. **Authority regulations** for which non-compliance can also be classified as a failure can be derived from the bodies of rules (e.g. EC-GMP Guideline, CFR). Consider which document is a law and which represents a guideline only. Never use risk management procedures to justify not following the law. It is just as important! Yet, also consider the **state of the art**, since some regulatory requirements take this into account. However, it is not always easy to determine the state of the art. The documents from associations (e.g. ISPE **Baseline®** series, PDA technical reports or ISO standards) can provide some help. These documents describe principles of how pharmaceutical production companies should design technical systems today. Often regulators are involved, since these documents are created by experts. They provide a good guide to the current state of the art.

10.I.2.4 Step 4: Identification of Possible Failures, Consequences and Cause of Failure: Hazard Assessment (Risk Analysis)

After documenting all potential failures and their consequences and causes, they must be organized systematically. Many different causes of failures may often lead to one common failure. This same failure may have several different consequences. It is documented in a form to ensure traceability (figure 10.I-3).

10.F-4.xls

Risk analysis according to the FMEA method

Page 1 of 2

Equipment **Purified water** **Qualific. no.** **xxx**

Executed on

Participants

Authorisation operator Date Signature

Authorisation quality assurance Date Signature

					Planned technical system				
No.	**Processing step or facility component**	**Type of failure**	**Failure consequence**	**Cause of failure**	**Preventive or inspection measure already in place**	**Occurrence O**	**Severity S**	**Detection D**	**RPN**
10	Fittings	Dead space valves (ball valves) have been fitted	Microbiological growth	Insufficient planning	Inspect all fitted valves and their installation and take regular samples of water qualities	4	7	3	84
20	Pipes/fittings	Residual water remains in the pipework when this is emptied	Microbiological growth	Insufficient manual welding	None	5	8	8	320
30	Distribution	Build-up of laminar surface layer on pipe walls	Microbiological growth	Insufficient flow velocity in the system	Calculation of the overall system and measurement of Reynolds value	5	8	10	400
40	Distribution	Content of pipes is not clearly identifiable	Mix-ups are possible during repairs and maintenance work	No labelling	None	4	6	4	96
50	Generation	System exceeds conductivity	Water quality is out of specification (pharmacopoeia)	System function insufficient	Inspection of reference equipment:inline monitoring of conductivity and alarm notification if exceeded	4	8	2	64
60	Generation	Exceeding of conductivity is not reported	Water quality is out of specification (pharmacopoeia)	No alarm is reported	None	6	8	10	480
70	Reverse osmosis	Water stands for too long in the reverse osmosis unit	Microbiological growth	Intervals of running time for reverse osmosis are too long (planning, programming)	Check planning documentation to see whether standing time is < 4 h	4	8	8	256

Figure 10.I-3 Examples of an FMEA

10.F-4.xls

Risk analysis according to the FMEA method

Equipment **Aqua Purificata** **Qualific. no.** **xxx**

Executed on

Participants

	Improved technical system							
No.	**Measure**	**O**	**S**	**D**	**pot. RPN**	**Deadline**	**Responsible person**	**Comments/notes**
10	No further measures necessary	4	7	3	84	-	-	RPN < 100, therefore no measure is necessary
20	Supplier evaluation, testing of all welded parts using endoscopy and inspection of all welding certificates and sample parts	1	8	8	64	30.07.2005	H. D. Müller	
30	Analyse flow velocity and install inline flow meters	2	8	2	32	21.07.2005	J. K. Maier	
40	No measures necessary	4	6	4	96	-	-	Well trained maintenance/installation personnel;pipes to be labelled by an experienced and consistently accurate company
50	No further measures necessary	4	8	2	64	-	-	If an alarm is triggered, the further procedure is controlled by the relevant SOPs.
60	Test all quality-critical alarms covered by OQ; carry out a supplier audit in the area of controls (programming by system and program simulation)	2	8	2	32	20.06.2005	O. Anders	
70	Verification of conformance of process parameters with IQ and inspection of system function in terms of OQ	2	8	3	48	10.09.2005	H. D. Müller	

Key: O = Probability of occurrence; S = Failure severity; D = Probability of detection; RPN = Risk priority number

Figure 10.I-3 Examples of an FMEA

10.I.2.5 Step 5: Evaluation of the Failures and Determination of the Risk Priority Number (RPN)

As a general rule in the failure evaluation phase, only one line in the FMEA forms i.e. severity, probability or detection is evaluated at a time. If, for example, several causes of failure are listed in separate lines that are linked to one failure, only these failures must be considered individually. However, if the different causes of a failure are summarized in one line, the causes of the failure are evaluated together.

In general, the following aspects of failures are evaluated:
- Severity (S) of the failure consequence
- Probability of occurrence (O) of the cause of failure
- Probability of detection (D) if the failure occurs

These three failure characteristics are assigned numerical values, which are used to calculate the risk priority number (**RPN**) by multiplying the three values together (see figure 10.I-4).

$$RPN = O \cdot S \cdot D$$

O = Probability of occurrence, S = Severity, D = Probability of detection

Figure 10.I-4 Determining the risk priority number

A modified FMEA is also possible, in which the three evaluation criteria S, O and D are assigned a non-numerical classification such as "low" , "medium" and "high" . Also weight factors for S, O and D can be added. Sometimes a modification named as **FMECA** (*Failure mode effect and criticality analyses*) can be used.

It is essential that the three evaluations are performed independently of each other. For example, evaluation of the severity of a failure must not include its probability of occurrence or detection. If the consequences of a failure leads to, for example S = 8, it should not be reduced only because the failure only occurs once a year.

The possible value ranges (scope of the possible numerical values) of the individual failure characteristics must be established specifically by the company and adopted at the specific problem. Recently, a certain standard has also developed within the pharmaceutical industry by which the values from 1–10 are permitted for each failure characteristic.

However, it may be useful to restrict these value ranges for certain FMEAs e.g. only permit values from 1–4. An even number is always beneficial in order to omit the mean. When determining the possible value ranges, it is always important to develop evaluation guidelines before an FMEA is executed, so that the significance of the individual numerical values is defined e.g. what does a probability of occurrence of 3 mean?

It should be noted that this process might be time consuming. It has shown that the communication between the team members is always beneficial. Often, sufficient or adequate data is not available to define and select one of the 10 levels. Therefore, a 4 level approach is often more helpful, which might result in the decisions very high risk (e.g. level 10), high risk (e.g. level 7), low risk (e.g. level 4) and very low risk (e.g. level 1). Ask yourself whether it is more uncertain to rank a risk without sufficient correct data in a 1–10 scale of in a 1–4 scale, where you can be sure to be in the right level. Experience has shown that using a 1–10 or 1–4 scale will result the priorities to be similar. High risks will never get low.

Always keep in mind why it is necessary to do this: to enable the prioritization of hazards and consider actions based on a multifactor approach looking into the future (severity), including knowledge from the past (probability), and consider what can happen today (detection). Also, long discussions can occur while introducing weight factors. It is up to the skills of the moderator to drive the discussion on the context between the different disciplines, and to stop it if it's circulating.

Severity (S) of a Failure

The severity of a failure is an essential feature for this assessment. It refers to what may happen in the future. The severity of the failure is generally determined by the consequences of the failure. It should be clarified in advance, whether the failure of severity only affects the "end consumer" (patient), or whether the severity of the failure for the next "customer" should be considered e.g. internally the packaging area may be a customer of the tablet packaging area. The latter is usually the option, since it increases the stability of the processes and minimizes the business risks, which should be preferred e.g. as a result of unusable products that need to be destroyed. The numerical value increases from 1 to 4 (or 1 to 10) with increasing severity (figure 10.I-5).

Consider if such a 10 step approach is useful or if a lower number of discrete steps is enough to prioritize actions (figure 10.I-6).

When creating a guide for the evaluation of failure severity, it is useful to take into account the effects of a failure in terms of staff (including management), the environment and possibly data integrity issues.

Probability of Occurrence (O)

For a evaluating the overall risk, it is of high importance to determine how often a failure occurs or can occur. The more frequently a failure occurs, the higher the risk. This means, for example, that O = 1 might stand for a rare occurrence and O = 10 a very frequent occurrence. The probability of occurrence is generally determined by the cause of failure. It refers to the experience gained in the past and tries to predict the future (figure 10.I-7).

In the example above we can also directly see the problems that often occur when estimating probability of occurrence. In order to use this type of table, well-founded historical operating data must be available for a particular process or facility. If this historical operating data is not available, it can often be beneficial to reduce the level of detail by grouping together individual evaluations (figure 10.I-8).

Evaluation guide for failure severity		
Evaluation	**Classification**	**Explanation**
1	Very low	No adverse effects on product/process quality can be derived. The failure consequences are wholly insignificant.
2	Low	No adverse effects on product/process quality are likely to be derived. The failure consequences are insignificant.
3	Low	An applicable product can be expected. The master batch record is fulfilled, although some deviations in the process exist.
4	Low	An applicable product can be expected. The master batch record is fulfilled, although considerable deviations in the process exist.
5	Medium	The use of the product is limited (e.g. specification is borderline), process is stable.
6	Medium	The use of the product is limited (e.g. specification is borderline), slight deviations in the process exist.
7	Medium	The use of the product is limited (e.g. specification is borderline), process is unstable.
8	High	The product has to be rejected; damage to patient health cannot be excluded.
9	High	The product has to be rejected; damage to patient health cannot be completely eliminated. Process changed has to be considered
10	High	The product has to be rejected; damage to patient health is likely. Process must be changed

Figure 10.I-5 Example of an evaluation guide for failure severity using 10 levels

Rating	Possible Description	
	Safety	**GMP**
Extreme (Catastrophobic)	Effects, which are potentially life-threatening or could cause a serious risk to health or a temporary health problem and/or might trigger a potential recall.	Close down of site or drug shortage and/or consequences do affect quality and regulatory compliance of a product.
High (Critical)	Effects, which could cause illness or mistreatment but are not covered by equivalent examples of "rating catastrophic",	Consequences which indicate systematic errors GMP systems or product registration.
Moderate (Marginal)	Effects, which do not cause a serious risk to health no side effects, but patient ca observe the defect	Consequences, which indicate system problems of processing/handling, which might impact also other batches/products
Minor (Negligible)	Effects/complaints, which do not cause a risk to health.	Consequences, which effect local daily operations

Figure 10.I-6 Example how to rank severities for analyzing manufacturing processes using 4 levels only

Evaluation	Classification	Explanation
1	Very low	Failure frequency <0.01% or failure is not expected
2	Low	Expected failure frequency ≥0.01% and <0.05%
3	Low	Expected failure frequency ≥0.05% and <0.1%
4	Low	Expected failure frequency ≥0.1% and <0.2%
5	Medium	Expected failure frequency ≥0.2% and <0.5%
6	Medium	Expected failure frequency ≥0.5% and <1.0%
7	Medium	Expected failure frequency ≥1.0% and <2.0%
8	High	Expected failure frequency ≥2.0% and <5.0%
9	High	Expected failure frequency ≥5.0% and <10.0%
10	High	Expected failure frequency ≥10%

Figure 10.I-7 Examples of evaluation guides for probability of occurrence using the rating 1 to 10

Rating	Possible desription
Frequent	once per order or < 2 days
Repeated	once in 10 orders or < 2 per month
Occasional	once in 100 orders or < 4 per month
Unlikely	may be once in 1.000 orders or abaot once a year

Figure 10.I-8 Modified example of evaluation guide for probability of occurrence

It should initially be graded to highest risk (O = 10; *worst case*), if it is not possible to classify the probability of occurrence in this general evaluation, since no historical operating data regarding the probability of occurrence is available. As new information becomes available, this evaluation can be adapted.

Probability of Detection (D)

When evaluating hazards for determining risks, it is important to know whether a failure that occurred can be detected or will be noticed from the customer or the pharmacist later on.

The easier the failure can be detected the lower the risk. The numerical value thus decreases from 10 to 1 or 4 to 1, the higher the probability of detection is. This would mean that D = 1 is a value that, for example, can only be achieved if a fully automatic 100% test is integrated in the process or production process flow or that the failure is really obvious. D = 10 or 4 means that a failure is most probably not detected. Note this is an inverted scale due to severity and probability. The probability of detection is generally determined by the cause of failure (figure 10.I-10, figure 10.I-9).

Rating	Possible desription
Normally not detected	Failure very likely to be overlooked, hence not detected (e.g. no technical control, no manual or visual control)
Repeated overlooked	Failure may be detected (e.g. audit as spot check, Monitoring)
Occasional been overlooked	Failure detected by procedure in place
Unlikely to be overlooked	Failure immediately identified

Figure 10.I-9 Example of an evaluation guide for probability of detection using 1–4 scale

Evaluation guide for probability of detection		
Evaluation	**Classification**	**Explanation**
1	Very low	The failure is detected in 100% of cases; automatic measuring/test system, 100% control, and process is halted immediately when failure is detected.
2	Low	The failure is detected in 100% of cases; automatic measuring/test system, 100% control.
3	Low	The failure will most probably be detected; automatic measuring/test system, random sample control, process is automatically halted, if failure is detected
4	Low	The failure will most probably be detected; automatic measuring/test system, random sample control (>20%).
5	Medium	The failure will most probably be detected; manual 100% control (e.g. test system, test tools are in place).
6	Medium	The failure will probably be detected; visual 100% control
7	Medium	The failure can be detected; manual control (>20%) test system, test tools, etc. are in place).
8	High	The failure can be detected; visual control (> 20%).
9	High	The failure can be spotted visually at random; sporadic visual test or monitoring.
10	High	The failure is not detected (no control).

Figure 10.I-10 Example of an evaluation guide for probability of detection using 1–10 scale

When evaluating the probability of detection, the test measures in particular that are already planned or designed at the time the FMEA is executed must be taken into account. If this is the case, they must be documented in the FMEA form together with the evaluation.

For example if detections are related to an analytical method e.g. in a tablet packaging process and if the completeness and integrity of tablets in blisters is constantly monitored by a control camera, it should be included in the evaluation. In this example, the probability that empty blisters will be detected increases, (proper functioning of the camera must be proven during qualification of the equipment), and hence the risk priority number decreases.

Evaluation of the Risk Priority Number (RPN)

The risk priority number RPN is calculated by multiplying the values S, O and D.

This results in a RPN between 1 and 100 while using the evaluation numbers 1–10 as described above. In addition to the RPN, the problem's own risk tolerance is also highly significant. This also will differ from company to company and may be judged by regulators. It is the level at which the management sets the limits for determining measures. It also means that the management decides when a risk is acceptable or not. The management needs to clarify, which RPN represents the critical level above which risk-reducing measures need to be implemented. You need to establish whether this should be just one limit or more, for example, two (see figure 10.I-11).

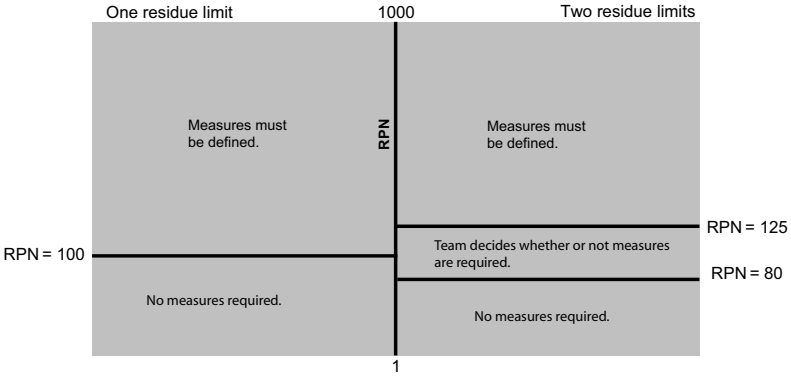

Figure 10.I-11 Example for determining RPN limits

A threshold can also be determined by looking at the S, O and D values independently. Consider which level would be accepted and which not. The threshold is created by multiplying the lowest unacceptable levels.

Using pre-defined thresholds is entirely arbitrary. It encourages "tick-box" compliance mentality and "fixing numbers" to meet pre-defined threshold. It is more important to make judgements based on relatives not the actual magnitude of the RPN. Often you can see a natural clumping of RPNs. Scales are hard to develop and you need to try them and improve them. However do not spend too much time arguing about an exact number. The numbers are not important; the relativities are. Also there should be a sense kept of realism. The process of RPN enables comparison of risk levels and does not give absolute magnitude of risk.

However, FMEA as a structured risk assessment tool helps to determine comparative levels of risk. Thus, the absolute value of the RPN is not important, and a natural clumping of RPNs can often be observed. It is important to make judgments based on relativities not on the actual magnitude of the RPN.

10.I.2.6 Step 6: Definition of Reduction Measures

If the set limits are exceeded, the FMEA team needs to define measures that lead to a reduction of the overall RPN to an acceptable level, or to accept the residual risks. Consider measures to be taken for every unacceptable risk to reduce the consequences, probability or detection or both. The reduction of consequences should always be the primary means.

As aids on how to challenge possible actions you may consider the following:

1. Technical measures
2. Organisational measures
3. Personnel measures
4. Emergency planning

All planned measures, including the planned implementation dates and responsibilities can be documented in a FMEA form.

As a result of the planned measures, the RPN should be re-evaluated (RPNpot = expected RPN after action implemented). The result is known as the potential **RPN**, meaning the RPN that can be expected on completion/implementation of the planned measures (figure 10.I-12).

$$RPN_{pot} = S_{pot} \cdot O_{pot} \cdot D_{pot}$$

RPN_{pot}: potential risk priority number,
S_{pot}: severity of the failure,
O_{pot}: potential probability of occurrence
D_{pot}: potential probability of detection

Figure 10.I-12 Calculation of the potential risk priority number

Some examples of suitable measures for reducing the probability of occurrence and increasing the probability of detection are listed below:

- Changes to facility to completely prevent the occurrence of the failure,
- design redundant systems,
- testing of certain functions during system qualification,
- implementation of additional in-process controls or process analytical technology (PAT),
- staff training[1],
- introduction of additional test points as part of preventative maintenance,
- introduction of organizational regulations (standard operating procedures).

The results after implementing actions can be visualized. See an example for an overview of levels of risk reduction in the upcoming figure 10.I-13.

1. Consider the consequences; training is not always the right measure for reducing risk

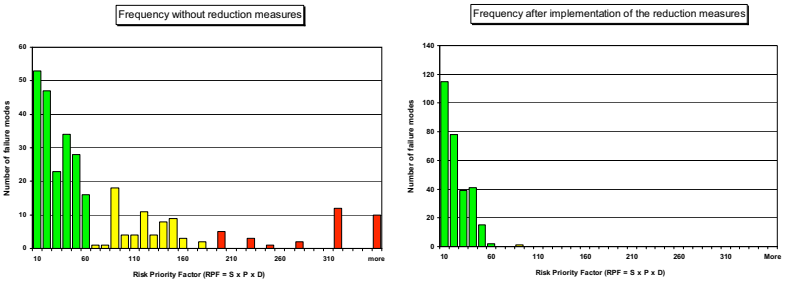

Figure 10.I-13 Show levels of risk reductions after implementing actions

Further Parameters for Assessment of the Overall Process

Additional parameters that can be derived from an FMEA include the average RPN and the overall potential of a process. The average RPN is a parameter for evaluating the overall process. It can be used to provide a direct comparison between individual processes in terms of anticipated risks (figure 10.I-14).

$$\overline{RPN} = \frac{\sum RPN}{Number}$$

$\overline{RPN}$: average risk priority number

$\sum RPN$: total of individual risk priority numbers

Number: number of risk priority numbers available

Figure 10.I-14 Calculation of the average risk priority number

The overall potential specifies the amount by which the average RPN is expected to be reduced after implementation of all planned measures (figure 10.I-15).

$$\overline{RPN}_{Overall\ Potential} = \overline{RPN}_{Initial\ state} - \overline{RPN}_{Pot.}$$

$\overline{RPN}_{Overall\ Potential}$: overall potential,

$\overline{RPN}_{Initial\ state}$: average risk priority number of initial state (without determining measures),

$\overline{RPN}_{Pot.}$: average potential risk priority number

Figure 10.I-15 Calculation of overall potential

All this requires additional affords. The company has to decide case-by-case if this is of added value. Maybe try it once, and keep it away, if it does not show a benefit.

10.I.2.7 Step 7: Awareness of the Residual Risks

If the potential RPN is at this stage a decision is required, if after definition of measures, is still higher than the limit, while involving the management on whether the process or facility should be implemented or retained with the residual risk.

However, scales are hard to develop. You need to try them and improve them. Do not spend too much time arguing about an exact number. Keep in mind: the numbers are not important; the relativities are. This leads to the essence to keep a sense of realism. The FMEA process enables comparison of risk levels; it does not give an absolute magnitude of the risk. Within larger projects, individual measures may often need to be adapted and re-evaluated. In these cases, the FMEA needs to be revised and new versions of the FMEA prepared.

10.I.2.8 Step 8: Summary of the Results

When running a FMEA a large amount of data, knowledge and of causes will be gathered. Therefore, an executive summary may be helpful. It should be made up of 1–2 page(s) only.

See some possible elements e.g.

- Which tool(s) were used
- Process steps with "potential high risks"
- Topics for corrective / preventive actions as an overview
- Overview of the level of risk reduction (e.g. chart)
- List of accepted residual risks
- Refer to detailed documentation
- Approvals for commitment to agree and endorse the actions e.g. Senior Management (e.g. manufacturing, QA)

10.I.2.9 Step 9: Documentation of the Performed Process

A detailed documentation of the risk management summary could be archived for the records.

10.I.2.10 Step 10: Follow Up and the Implementation of Measures

In order to guarantee that the planned measures will be implemented, a designated member of the FMEA team should control/monitor the deadlines and implementation of all measures.

These have to be done within the management responsibility to review progress considering the performance of the defined and agreed actions. Another follow up can be done during the training of new managers. They can use the FMEA to learn from the knowledge gained by the risk management team.

In an ideal case, a FMEA is a "living" document by modifying or adding continuously new events, causes, effects and the follow up of actions e.g. after being dis-

covered by a deviation/investigation process, as result from audits / inspections. A FMEA should be used as a management and knowledge instrument. There is no need to revisit a FMEA periodically within a defined time frame.

10.I.3 Implementation of FMEA in a Project

It has been shown beneficial to not run long theoretical training sessions, but to perform and run practical examples to the staff. If a separate project is needed, or if there are skills available within the staff to implement it, it should be done step by step.

The implementation of a risk assessment and control in accordance with the FMEA method requires meticulous planning. A checklist is provided as an example, in which all important points for a successful implementation are listed in chronological order. The timeframe in which the individual points are to be processed is a project planning task for the implementation of a FMEA project (figure 10.I-16).

10.I.4 Advantages and Disadvantages of an FMEA

The FMEA as a methodology offers many advantages, which show that the FMEA has ultimately prevailed in many industry sectors in preference to other methods of risk assessment and control activities. The advantages of an FMEA include the following e.g.

- Semi quantitative evaluation of risks
- Ranking of risks and proactive disclosure is possible
- Qualification aspects are defined at an early stage
- Various levels of assessment are possible
- Interdisciplinary teams
- Traceability of decisions
- Evaluation guide for subsequent process/product/system changes
- Comprehensive method, also suitable for non-GMP risks

Semi Quantitative Evaluation of Risks

The FMEA can provide a semi quantitative evaluation of risks. In the form described here, these results in a risk priority number (RPN), whereby the risk increases as the numerical value increases. The team itself can define at which level the acceptable risk and thus a limit is set. Often a clubbing of the low, medium and high risks is observed so that the limits are obvious. The risk priority number (RPN) can be used to compare risks between processes, if the same evaluation criteria are used, and also between different technical systems. This enables the available resources to be concentrated on the processes/systems with high risks and residual risk to be minimized.