A Guide to Supply Chain Risk Management

for

Suppliers to the Pharmaceutical, Medical Device and Allied Industries

Second Draft for Consultation

28th May 2009
Copyright

Pharmaceutical Quality Group

Acknowledgements

Specific acknowledgements are given for the contributions of the following people:

A list of contributors will be included in final document.

Please Note

The authors would like to remind the reader that the guidance given here is advisory and illustrative only. It is recommended that users supplement their understanding of Risk Management from some of the publications listed in Annex 3 – References and bibliography.
## Contents

<table>
<thead>
<tr>
<th>Ref</th>
<th>Title</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>0</td>
<td>General Introduction</td>
<td></td>
</tr>
<tr>
<td>Part 1</td>
<td>Implementing Risk Management</td>
<td></td>
</tr>
<tr>
<td>1.1</td>
<td>Introduction and guidance on Implementing Risk Management</td>
<td></td>
</tr>
<tr>
<td>1.2</td>
<td>Risk Identification</td>
<td></td>
</tr>
<tr>
<td>1.3</td>
<td>Risk Analysis</td>
<td></td>
</tr>
<tr>
<td>1.4</td>
<td>Risk Evaluation</td>
<td></td>
</tr>
<tr>
<td>1.5</td>
<td>Risk Reduction</td>
<td></td>
</tr>
<tr>
<td>1.6</td>
<td>Risk Acceptance</td>
<td></td>
</tr>
<tr>
<td>1.7</td>
<td>Risk Communication</td>
<td></td>
</tr>
<tr>
<td>1.8</td>
<td>Risk Review</td>
<td></td>
</tr>
<tr>
<td>Part 2</td>
<td>Risk Management Toolbox</td>
<td></td>
</tr>
<tr>
<td>Part 3</td>
<td>Risk Management Examples</td>
<td></td>
</tr>
<tr>
<td>Annexes</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Annex 1</td>
<td>Examples of different categories of supply</td>
<td></td>
</tr>
<tr>
<td>Annex 2</td>
<td>Glossary and Definitions</td>
<td></td>
</tr>
<tr>
<td>Annex 3</td>
<td>Bibliography</td>
<td></td>
</tr>
</tbody>
</table>
General Introduction to Supply Chain Risk Management

With outsourcing and global supply chains becoming more prevalent in organisations, it is increasingly important to build security into and throughout the supply chain. It is the responsibility of each purchaser to ensure that their suppliers provide materials and services of the appropriate quality throughout the lifecycle from design and development through to end-user.

This explanatory guide provides guidance on Supply Chain Risk Management supported by illustrative examples and suitable risk assessment tools. It does not introduce new concepts, rather it provides guidance on the practical application of existing Risk Management models to the supply chain. It is intended to support organisations with little experience in the area of Risk Management as well as to reinforce critical aspects of supply chain to those with more experience. It is consistent with currently developing industry standards and expectations.

The term “Supply Chain” includes all suppliers that are important to an organisation, its products and/or its services. The interface and relationship between and within organisations, their suppliers and suppliers to the suppliers is therefore key in understanding and identifying the potential risks to the quality of products/services and ultimately the safety of patients.

The scope of this guide is applicable to:

- suppliers to the pharmaceutical, medical device and allied industries (see annex 1);
- how suppliers manage risk within their organisation;
- how internal risk is managed within an organisation;
- how suppliers manage their supply chains; and
- the pharmaceutical, medical device and allied industries in assuring quality in supply to the end-user.

Supply chain risks have increased as a result of:

- materials shortage;
- reduced inventory;
- longer / more complex supply chains; and
- greater exposure to global, political and financial environments.

It is important to note that supply chains can vary from short and simple to long and complex. The time scale for some pharmaceutical products from receipt of a raw material through to finished product and supply to a patient, may take as long as 18 months.

Various problems can manifest themselves at any part of the product lifecycle, from the source of raw materials used to manufacture the product right through to the compliance of the patient using the product correctly. This can have an impact on products/services as well as business continuity, performance and security of supply. In order to protect the patient, it is important to identify potential risks, then assess and control them.
Diagram 1 - Pharmaceutical Supply chain showing Tiers

Diagram 1 shows the potential for supply chain complexity depicting tiers of supply. This highlights how suppliers far removed from the ultimate end user “the patient” can potentially have an impact.

Risk Management must have top management support and be an integrated part of the organisation’s business and quality management systems. Diagram 2 depicts Risk Management and its fit as part of good business practice using a lifecycle approach. This should help to enable timely and appropriate decision-making and ensure that, materials, products and services are of appropriate quality and are safe.
This guide is based on the pharmaceutical Risk Management model as represented in diagram 3. Risk Management is defined as a systematic process for the assessment, control, communication and review of risks across the product / service lifecycle. The level of effort invested may vary from case to case but essentially should be commensurate with the specific risk. The regulators have incorporated official guidance on Risk Management in European GMP Guide and have identified supply chain as an area of key concern.
It is in the interests of all stakeholders throughout the different tiers of the supply chain to manage risk effectively.

The level of risk can increase throughout the supply chain the closer the tier of supplier is to the end product / end user. However, risks created early on can perpetuate throughout the entire supply chain to the patient, and this can be compounded or increased through further processing. Although they present no obvious risks in the early stages, some hazards and their associated risks may not become apparent until too late! There are significant business implications associated with such events.

Note: Risk is a measure of an identified hazard (see glossary).

[LINK] – Example Heparin / glycerol
Global factors can also impact a manufacturer’s or supplier’s supply chain activities, with the organisation having little influence on the global factors at the root of the effect.

**[LINK] – Example Acetonitrile**

Some sources of supply chain risk are included in Table 1.

**Table 1 – Sources of Supply Chain Risk**

<table>
<thead>
<tr>
<th>External</th>
<th>Internal</th>
</tr>
</thead>
<tbody>
<tr>
<td>Increase / decrease in demand</td>
<td>Reject batch</td>
</tr>
<tr>
<td>Fluctuating exchange rates</td>
<td>Non conformance</td>
</tr>
<tr>
<td>Political climate / instability</td>
<td>Resource issues</td>
</tr>
<tr>
<td>Materials, product, service supply interruption</td>
<td>Supplier selection / qualification process</td>
</tr>
<tr>
<td>Unknown / poorly controlled use of brokers / agents</td>
<td>Use of contracts / agreements</td>
</tr>
<tr>
<td>Distribution problem</td>
<td>Facility disaster</td>
</tr>
<tr>
<td>Counterfeiting</td>
<td></td>
</tr>
</tbody>
</table>

Potential benefits of Risk Management

Applying the principles of Risk Management can:

- improve and develop business relationships between suppliers and customers;
- potentially reduce costs;
- minimise cost of compliance;
- improve business efficiency;
- increase confidence;
- reduce liability; and
- avoid waste and scrap.

Risk Management can help organisations safeguard the quality and supply of product / services to customers and ultimately the end user. It is about anticipating and controlling risk through an ongoing process of risk awareness, reduction / acceptance and review. This can help justify improvement / investment where needed and help prevent potential problems for customers (e.g. recalls, patient harm), and loss of business / closure.

Part 1 will cover the key steps of Risk Management providing guidance for users.
1.1 Implementing Risk Management

Risk Management should be an integrated part of any business and for successful implementation the following are key foundations:

- there must be top level management support and commitment;
- start simply and avoid complexity;
- look at internal and external risks;
- follow the cycle several times, learn, evolve and embed in the organisation culture.

Commitment by senior management is vital to ensure the process is viable and maintained and that valuable resource is invested and not wasted. Risk Management should not be considered as a one off project or event, but as the implementation of a mutually beneficial culture within and between organisations.

Diagram 4 - A typical supply chain for marketed products

Diagram 4 shows the various functional activities and the supporting services that may be involved in development and supply of product or service. An organisation may choose to outsource part or all of any of these activities. Organisations should consider all of their activities with respect to producing product or service and understand how their supply chains and interfaces work. This should apply throughout all phases of the product / service lifecycle (from design and development to routine manufacture, supply to customer and discontinuation).

The level of Risk Management awareness will develop over time with practice and experience. Table 2 illustrates the progression an organisation will make as they gain experience over time in the use and application of Risk Management. This is applicable to all categories of Risk Management and not just Supply Chain.
### Table 2 – Risk Management Maturity

<table>
<thead>
<tr>
<th>Risk Maturity Level</th>
<th>Risk Processes</th>
<th>Attitude</th>
<th>Behaviour</th>
<th>Skills &amp; knowledge</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Scepticism</td>
<td>No Formal Processes</td>
<td>Risk Avoidance</td>
<td>Fear of Blame Culture</td>
<td>Unconscious Incompetence</td>
</tr>
<tr>
<td>Awareness</td>
<td>Ad hoc use of Stand Alone Processes</td>
<td>Suspended Belief</td>
<td>Reactive, Fire fighting</td>
<td>Conscious Incompetence</td>
</tr>
<tr>
<td>Understanding &amp; Application</td>
<td>Tick Box Approach</td>
<td>Passive Acceptance</td>
<td>Compliance, reliance on registers</td>
<td>Conscious Competence</td>
</tr>
<tr>
<td>Embedding &amp; Integration</td>
<td>Risk Management embedded in Business</td>
<td>Active Engagement</td>
<td>Risk-based decision making</td>
<td>Unconscious Competence</td>
</tr>
<tr>
<td>Robust Risk Management</td>
<td>Regular review &amp; Improvement</td>
<td>Champion</td>
<td>Innovation, Confident Risk taking</td>
<td>Expert</td>
</tr>
</tbody>
</table>
1.2 Risk Identification

Purpose

The purpose of the Risk Identification stage in the overall Risk Management process is to determine “What Can Go Wrong?”

Risk Identification is defined as “a systematic use of information to identify hazards referring to the risk question or problem description.”

Risk Identification importantly represents a starting point in the Risk Management process and forms the foundations for the remaining stages of the process. The potential hazards identified as outputs from the Risk Identification stage are then subject to examination in detail during the Risk Analysis and Evaluation stages.

Input

Risk Management requires information about the process to be assessed. The scope if not already defined should be determined to ensure the team stays focused and resource is not wasted. Determining the limits of the Risk Identification stage will help to define what data / information may be relevant or should be examined to identify potential hazards.

In terms of supply chain the following should be considered:

- each supplier within the whole supply chain and what they supply (material / product / service);
- the structure of the supply chain and interfaces (between / within organisations, their suppliers and suppliers to the suppliers);
- what is supplied (material / product / service);
- internal processes that manage the suppliers;
- internal product realisation processes.

Data / information can take many forms, for example:

- quantitative data/information - numbers, figures, measurements and variables;
- qualitative data/information – attributes (yes/no, go/ no go);
- soft data/information – subjective / historical / experience / process complexity and interactions between processes

Many professionals and organisations often fall into the trap of assuming all good information takes the form of formalised (hard) quantitative and qualitative data / information. Although this information is valuable and easily evaluated, soft data/information should also be considered. See diagram 5 for sources of information.
Diagram 5 - Sources of Information that can be used in Risk Identification

- **Data / Information**
  - **Hard Data/Information**
    - Facts
    - Measurements
    - Analysis results
    - Trends
    - Variables
    - Attributes
  - **Soft Data/Information**
    - Observation
    - Experience
    - Assumptions (Gut Feel)

**Key**

- = Qualitative
- = Quantitative
- = Both

It is fundamental that the people who best understand the process under assessment are consulted to ensure accurate and complete information. It is recommended that Risk Identification is undertaken by interdisciplinary teams (people with the necessary expertise representing relevant operational functions within the organisation or supply chain). Involvement of individuals may vary from stage to stage. Note that in smaller organisations / supply chains this may be limited to just a couple of people. Consider the example which illustrates the importance of having the right team.

**LINK – Example – selecting right team**

**Process**

Risk Identification is concerned with assessing information. Whatever the activity to be assessed, it is recommended to map out the process concerned (key points / factors) and ask the question “what can go wrong?” repeatedly. This enables potential risk areas to be easily identified, agreed and visualised by the appointed interdisciplinary team. It is important for completeness to ensure that interfaces between processes are also identified as this is where problems can go unnoticed.

**LINK – Toolbox – Process Mapping**
Other common approaches to Risk Identification are included in the Risk Management Toolbox.

Any known risks should also be incorporated. Risk Identification provides an opportunity to place known hazards / risks into context for the evaluation stage. Known risks result from various sources such as (not exclusively):

- deviations / non-conformances;
- near miss events (valuable source of potential risk areas);
- complaints;
- internal / external audits;
- critical Process Parameters (CPP) / Key Performance Indicators (KPI);
- components of the process under assessment i.e.:
  o people, premises, equipment, materials;
  o QA/QC;
  o services;
  o utilities;
  o environmental factors;
  o logistics.
- knowledge in the public domain (e.g. news, regulatory actions, legislation, etc).

Output

The output of the Risk Identification stage of Risk Management is a list of known and potential hazards for the process reviewed based on information available at that time. There is no guarantee that all hazards / risks can be identified at any given time. It is important to understand that processes may change and other events may influence the outcome and will require review and reassessment. Depending on the Risk Identification tool used and the extent of the assessment, potential risks may be categorised prior to analysis e.g.:

- product quality risks;
- business risks;
- risks associated with raw materials;
- risks associated with machinery;
- risks associated with people etc.

At completion of this step there should be confidence in answering the question “What can go wrong?” for the process under assessment. At this stage risks will not be evaluated as critical or non-critical as this level of risk understanding will be achieved through the Risk Analysis and Risk Evaluation stages.

Note: be aware that there will be unidentified or unidentifiable risks to the organisation.

The output from Risk Identification should be agreed, documented and communicated to relevant stakeholders.
1.3 Risk Analysis

Purpose

This step of the Risk Management process attempts to estimate the level of the identified hazards / risks in terms of severity of harm, likelihood of occurrence and detection. It provides us with either a quantitative or qualitative estimate of each risk.

Input

Prerequisites

In order to perform an analysis of the hazards / risks, the Risk Identification step must be complete. There should be sufficient confidence that at least the significant hazards / risks have been captured from both business and quality Risk Identification exercises.

Before starting, it is necessary to be clear as to what the scope of the analysis is (e.g. each supplier, the whole supply chain or each product) and to decide upon the most appropriate risk analysis tool to use. There are a number of different possible tools to use but the choice depends upon the level of experience and expertise of the user, as well as the suitability of the tool to make an effective decision.

Considerations

The primary options are to use either a “qualitative” tool such as risk ranking etc or to use a “quantitative” tool such as Failure Mode & Effects Analysis (FMEA), Cause and Effect matrix (C&E), etc.

- A qualitative estimate is one where there will be a descriptive expression of the level of risk after the analysis, for example low, medium or high;
- A quantitative estimate is one where there will be a numerical score or other detailed measure of the risk after the analysis;
- A combination of the above two approaches.

Where possible, hard data rather than soft data (subjective opinion) should always be used in order to provide greater confidence in the outcome. However, so that a specific Risk Assessment tool will function, it may be necessary for soft data to be translated into numeric values.

The relevant operational experts should provide detailed and up-to-date knowledge of current and historical performance. Where knowledge does not exist or data is unavailable, then this should be sourced in the long-term. In the short term, best estimates can be made on the basis of assumptions provided these are clearly identified. Significant decisions based on subsequent recommendations should always reference the assumptions made and further review be scheduled.

An example of subjective assessment:

A company does not have a supplier complaints system. The logistics manager knows that Supplier X is the worst offender for late deliveries because the logistics team are always complaining about them. However, the logistics manager probably does not know how they compare with Supplier Y based on a percentage of volume, a difference, or what the related costs are. This demonstrates a gap in the organisation’s systems and supplier performance metrics / data.

Choosing which one to use should include considering several factors indicated below:
Whilst the diagram above may be seen as an oversimplification, it is meant to be a guide to the pros and cons of different types of Risk Analysis tools.

Table 3 - Pros and Cons of the tools

<table>
<thead>
<tr>
<th>Tool</th>
<th>Pros</th>
<th>Cons</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Qualitative</strong></td>
<td>Quick Can use soft data / opinion Limited training needed</td>
<td>Output is inaccurate Does not differentiate well between levels of risk</td>
</tr>
<tr>
<td>e.g. Risk Ranking (3 x 3)</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Semi quantitative</strong></td>
<td>Differentiates better between risks than the Qualitative approach Good balance of Pros and Cons of the other tools</td>
<td>May not be good enough for a mature Risk Management process</td>
</tr>
<tr>
<td><strong>Quantitative</strong></td>
<td>Output is accurate and precise Differentiation between risks is precise Includes detectability assessment</td>
<td>Relies upon hard data Training and experience are needed Confusion often occurs between failure mode and effect Takes time to perform, especially the first time Reliant upon experts to agree scores for S, O &amp; D</td>
</tr>
<tr>
<td>e.g. FMEA</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Ultimately the decision of which Risk Analysis tool to use depends upon:

- the risks identified
- the precision of the data or opinions that define the risks
• what tools customers / suppliers use;
• how accurate the output needs to be; and
• how quickly the output is required.

It is common for accurate or precise data to be missing in one or more areas, allowing the expert in
that area to “have a feel for” the level of risk but not be able to support opinion with factual evidence
or data.

It is recommended that where an organisation has little or no experience of any particular tools, or are
not required by customers to use a certain tool, then they use a qualitative tool. Once expertise in the
tool has been gained and supporting systems established, then the organisation can progress with
the use of increasingly more quantitative tools. This approach means that for the same investment of
time (at each repetition of Risk Analysis) an increasing percentage of time is dedicated to improving
the confidence of the risk estimation and therefore adding more value each and every time.

Different Risk Analysis tools are more appropriate than others for certain situations. For example
consider the pros and cons of the following:

Process

Having identified the risks and decided on the Risk Analysis tool to be used, the next step is to assign
a rank or score to each of the identified risks. An interdisciplinary team with knowledge of the
identified risk areas should agree ranking or scores for each one (following the rules and guidance for
the tool being used).

If necessary input can be provided remotely, but this is only effective where hard data is available and
is being entered or converted into a risk level. Where opinion / soft data is being used, agreement
through discussion and compromise is necessary.

Every risk identified must be assessed using the same Risk Analysis tool and at the same time / same
stage of the risk management process.

Note that Risk Assessment can be initiated and performed on an ad hoc basis (not as part of the
routine periodic cycle of Risk Management) when external or internal events occur. At such times, the
generation of a Risk Assessment level / score will enable the correct evaluation and risk acceptance /
mitigation decision to be made. Rapid escalation and communication of the Risk Analysis output
should occur for any confirmed high risks.

Link to Risk Communication

The use of ad hoc, reactive risk assessments is commonly used in Quality Departments to help make
and support decisions e.g. deviations, non-conformances, complaints.

Output / deliverable

A level or a score for each identified risk must be generated and documented. It is essential that this
output is communicated to those responsible for the Risk Evaluation step enabling this to occur in a
timely manner.

Note that where ad hoc assessments are made, immediate communication should be performed for
any confirmed high risk events.

References and examples to support

Examples of the risk analysis tools are provided in …….
1.4 Risk Evaluation

Purpose

“Risk Evaluation compares the identified and analysed risk against given risk criteria”.

Risk Evaluation is the process that organises the information from Risk Analysis and which allows the decision making step of Risk Reduction or Risk Acceptance to be made. To achieve this, a level of tolerable risk must be defined against which the Risk Analysis output can be compared.

Input

The prerequisites for this step are that:

- Risk Analysis has been completed;
- data is organised in the most appropriate way according to the Risk Analysis tool used; and
- a tolerance level has been set that the output from the Risk Analysis can be compared against.

This process is generic to all Risk Management activities and not just Supply Chain.

The “level of tolerable risk” depends on the product or service and the criticality of its application. However this should be set in a logical and scientific way. A simple way of setting the “level of tolerable risk” is to choose the highest group or most frequent type, e.g. all the Red / High risks OR to create a Pareto chart and select the top 20% (and hopefully cover 80% of issues). The method for setting this level should be documented so that it can be explained, justified and evolve over time.

In order to compare the Risk Analyses against an agreed “level of tolerable risk”, it is easier to rank these / sort these in order of descending risk.

Link to Tool box - simple Risk Ranking Matrix

By scaling the Low / Medium / High risks to a simple arithmetic scale, the combination of probability and severity can be evaluated, by simply multiplying the factors. The potential risks which have a higher score (i.e. 6 or greater) therefore carry a higher potential risk.

More sophisticated models for setting the “level of tolerable risk” exist. For quantitative Risk Analyses such as FMEA (IEC 60812), individual acceptance criteria may need to be established for each element. For example, borderline tolerance levels can be set at various steps in the Risk Analysis process, and the cumulative score of these determined. Minimum acceptable scores for each of Severity, Occurrence and Detection when multiplied will give a tolerable Risk Priority Number (RPN).

This example has certain weaknesses and so the value of experience should not be underestimated. Setting a “level of tolerable risk” is probably the step where both experience and evolution of the Quality Risk Management process can provide most value.
The Risk Analysis output must be organised (filtered, ranked etc) so that those which are most significant (i.e. above the level of tolerable risk) are identified.

**Link to Tool Risk Evaluation simple “Low/Medium/High” model and a simple matrix.**

Although a sense check of the information / data may have been performed already in the Risk Analysis stage, anomalous results can often be detected more easily in this stage. For example outputs that look too high or too low can be checked for calculation errors, missing data, incorrect data and then either be corrected or the result be verified as being accurate.

Finally this step categorises the risks into those that are above or below the level of tolerable risk. Failure to perform this step correctly can lead to poor decision making at the Risk Reduction and Acceptance steps.

**Output**

No final decision is made in this step. The output is two data sets (above and below the tolerance level) that can be checked further or be used as the basis for either Risk Reduction or Risk Acceptance.

The output should be communicated to relevant stakeholders including the Risk Control owner. Formal records should be retained for a suitably defined period to provide evidence as the basis for decisions made and enable ongoing reiteration / review.
1.5 Risk Reduction

**Purpose**

Risk Control encompasses the decision-making activities that result in action (Risk Reduction) or inaction (Risk Acceptance).

- Risk Reduction: To agree to take actions that reduce or avoid the identified risks, including the allocation of resource and investment, where appropriate; and
- Risk Acceptance: To agree not to take other actions and to accept the level of risk associated with such decisions at this time.

The Risk Reduction step focuses on processes for control or avoidance of risks where it exceeds a specified or tolerable level. Having evaluated the risks as part of the Risk Assessment step (Risk Identification, Analysis and Evaluation) and decided which the most significant risks are, appropriate decisions need to be taken.

**Input**

Ensure that the Risk Assessment phase is completed before proceeding. Setting an agreed tolerance level for risks and creating two data sets (above and below the tolerance level) is the output from the Risk Evaluation step. The inputs for the Risk Reduction and Risk Acceptance processes are as follows:

- output of Risk Evaluation;
- additional or new information identified;
- key decision makers.

**Process**

Where risks have been evaluated as requiring action, a decision has to be made as to whether it is feasible both technically and economically and safe to reduce this risk, and whether the company (or its stakeholders) require this risk to be controlled.

It is important to note that at this stage several theoretically possible solutions to reduce or eliminate risks may be identified, but that not all actions will be practical to implement in either a reasonable timeframe or at a reasonable cost or even be technically possible. At this point, the principles of ALARP (As Low As Reasonably Practical) are usually applied. Some actions may be possible or preferable to others, and these may reduce the risk to an acceptable level (see Risk Acceptance section).

When determining actions it is important to consider the following with input from the relevant experts such as:

- available resources;
- capability (organisation, suppliers and suppliers to suppliers); and
- policy (EHS, quality, finance and ethics).

There may also be both primary and secondary risks, where for example the supplier may be the primary risk and their supplier may be a secondary risk.

Risk Reduction actions that are identified for implementation should be considered in terms of their impact on the overall Risk Management process. Consider the following questions:

- are any new risks introduced as a result of the identified risks being controlled?
A Guide to Supply Chain Risk Management for Suppliers to the Pharmaceutical, Medical Device and Allied Industries

- is one significant risk being replaced with another?
- should another reiteration or part of the Risk Assessment process be performed?

Output

Decisions and actions relating to Risk Reduction must be documented and approved. Approval should endorse resource allocation, timelines and implementation strategy. This should be communicated.

Examples of reducing risk in the supply chain:

- define / map the supply chain to provide visibility of controls and bona fides of materials and services;
- implement robust supplier qualification process;
- implement a supply contract to ensure consistent supply and costs;
- implement a quality agreement or technical agreement to ensure responsibilities are clearly defined and understood by all parties with clear specifications;
- ensure that the supplier understands what the materials they supply are used for;
- have regular meetings between both parties to ensure effective communication, better understanding and cooperation in making improvements and controlling risks;
- influence supplier to ensure that they develop a proactive risk management process;
- implement metrics / key performance indicators that are tracked by both parties
- identify and implement a second source of supply that is not subject to the same risks as the original source of supply e.g. does not manufacture in the same region, does not have the same suppliers or is not subject to the same energy or transport limitations;
- identify and implement replacement suppliers where the existing supplier is not capable and cannot be improved in an acceptable timeframe

Different strategies can be applied to manage and control risk.

For example the supply from one company to another can be disrupted or cease in the event that the original site of manufacture closes. The transfer of production to another site where the material / product has not been made before presents a potentially great risk to the business. Technically it is possible (unless the skills and knowledge have been lost) but economically this may not be appropriate if the sales volumes are too small in the future to be viable. The supplying company might choose to discontinue the product unless the client company can either invest or move to another company. In this way the decisions of one company on both economic and technical grounds can present a significant and direct impact on customers and their ability to function.

Where the impacted company is a pharmaceutical manufacturer, the risk is not only one that could prevent manufacture, but could require lengthy and costly changes to the product licence. Delays in supply to the market could result in severe criticism or fines from the regulatory authorities where this endangers the lives of patients.

In many cases, the ways of reducing risk are simple and do not have significant costs, if these are identified and planned for in sufficient time. Costly risk reductions are usually the result of insufficient planning or insufficient cooperation with customers and suppliers. This is analogous to calling an emergency plumber when your boiler breaks down, as compared to the cost of an annual service or planning to replace the old boiler at the same time as replacing the kitchen.
1.6 Risk Acceptance

Purpose

The purpose of Risk Acceptance is to formally record the decision by senior management and communicate to the business and relevant stakeholders.

Input

Risk Evaluation should have been completed and the list of risks above tolerable level should have undergone Risk Reduction.

As part of any information gathering phase of an assessment, before taking decision to accept or reject, the following questions should be considered:

- are the right people involved?
- has anything been missed?
- is all the information available?
- are the assumptions really valid?
- have the right tools been used?

Process

Once the risks are understood and appropriate actions proposed, a formal review should be performed. This review has two specific purposes:

- Risk Reduction: To agree to take actions that reduce or avoid the identified risks, including the allocation of resource and investment, where appropriate; and
- Risk Acceptance: To agree not to take other actions, and to accept the level of risk associated with such decisions at this time.

Risk Acceptance is a decision by an organisation to continue to operate without any action to reduce a given risk on the grounds of either:

- the risk was below the tolerable level (either before or after risk mitigation or avoidance);
- the risk cannot be reduced at this time.

Reduction in risk is beneficial and to be encouraged, however there may be circumstances where there is no “reasonably practicable” way of reducing it, for example due to lack of technology etc. In such cases there may be little alternative but to accept the risk or look at other ways of reducing it. Being aware of risks at least enables a company to monitor the situation and be more able to react in an appropriate way should the situation change.

In terms of supply chain management, Risk Acceptance is a decision to initially use or continue the use of a supplier post qualification.

Output

Once the consequences and costs of any action or inaction have been explored and accepted as being appropriate, then these need to be formally communicated within and between the respective organisations. Records should be maintained.

The continued acceptability of risks from this stage should be incorporated as part of Risk Review. References and examples to support
### 1.7 Risk Communication

#### Purpose

Effective internal and external communication is critical to the success of any Risk Management process. Communication and consultation with internal and external stakeholders as far as necessary should take place at each stage of the Risk Management process. A plan to communicate and consult should be developed at an early stage to manage issues relating to the risk itself, its consequences and measures being taken to manage it.

Effective communication ensures that those accountable for implementing Risk Management and stakeholders understand the basis for decisions and outcomes of each stage in the process. Applying good communication practices increases the security of the supply chain.

The potential benefits of good communication practices to organisations, their suppliers and suppliers to suppliers are listed in Table 4 below.

#### Table 4 – Potential Business and Quality Benefits

<table>
<thead>
<tr>
<th>Business Benefits</th>
<th>Quality Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Ensures interests of stakeholders are understood &amp; considered</td>
<td>• Secure supply of products / services</td>
</tr>
<tr>
<td>• Increase security of supply chain</td>
<td>• Risk-focused quality management</td>
</tr>
<tr>
<td>• Secure business continuity</td>
<td>• Timely / effective end user protection</td>
</tr>
<tr>
<td>• Avoidance of financial loss</td>
<td>• Consistent conformance to specification</td>
</tr>
<tr>
<td>• Timely delivery of business impacting information</td>
<td>• Empowers continuous improvement</td>
</tr>
<tr>
<td>• Increased awareness &amp; understanding</td>
<td>• Enhances change management</td>
</tr>
<tr>
<td>• Improved planning through knowledge</td>
<td>• Promotes quality by design approach rather than quality by detection</td>
</tr>
<tr>
<td>• Improved resource allocation</td>
<td>• Brings functional experts together to identify and analyse risks</td>
</tr>
<tr>
<td>• Improved effectiveness &amp; efficiency</td>
<td></td>
</tr>
<tr>
<td>• Enhances mutually beneficial business relationships</td>
<td></td>
</tr>
<tr>
<td>• Enhances change management</td>
<td></td>
</tr>
</tbody>
</table>

Determining which communication practices to use is best decided by considering the who, what, when and how as illustrated below..
Who?

The first step in any successful communication process is to identify the relevant stakeholders. These will be the individual parties, groups and/or functions who:

- have an impact (direct or indirect) on the product / service;
- have an interest in your activities or project;
- must act on the outputs of the Risk Management process.

These stakeholders need to be identified and included where and when necessary at each Risk Management stage. Not all information needs to be communicated; it should be appropriate and relevant to the recipient. It is useful to appoint someone responsible for communication and this should be defined. Note confidentiality, contractual and regulatory obligations must be respected at all stages.

A RACI matrix is a useful tool to use in defining roles and responsibilities that is commonly derived from the four key responsibilities typically used, such as (Responsible, Accountable, Consulted and Informed). Table 5 below describes these roles. A matrix can then be defined for the Risk Management process so that it is clear to everyone who is responsible.

Table 5 – RACI roles and responsibilities

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Responsible</td>
<td>Those who do the work to achieve the task. There is typically one role with a participation type of Responsible, although others can be delegated to assist in the work required.</td>
</tr>
<tr>
<td>Accountable</td>
<td>Those who are ultimately accountable for the correct and thorough</td>
</tr>
</tbody>
</table>
### A Guide to Supply Chain Risk Management for Suppliers to the Pharmaceutical, Medical Device and Allied Industries

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>(also Approver / Final Approver)</td>
<td>completion of the deliverable or task, and the one to whom Responsible is accountable. In other words, an Accountable must sign off (Approve) on work that Responsible provides. There must be only one Accountable specified for each task or deliverable.</td>
</tr>
<tr>
<td>Consulted</td>
<td>Those whose opinions are sought; and with whom there is two-way communication</td>
</tr>
<tr>
<td>Informed</td>
<td>Those who are kept up-to-date on progress, often only on completion of the task or deliverable; and with whom there is just one-way communication.</td>
</tr>
</tbody>
</table>

The diagram below illustrates some key parties that could be included:

---

### What?

Depending on where in the risk management process you are then the information to communicate as an input or output changes. This will also influence the who, when and how factors of the communication activity.

Communication can be formal or informal. This will depend on the following:

- needs of the parties involved;
- nature of the inputs/outputs (e.g. data, information); and
- timelines & urgencies.
Important points can be captured in meeting minutes but key decisions should be formally documented to permit traceability and review.

The type of information to communicate may be determined using a variety of basic tools including brainstorming and gap analysis techniques.

**Link to Toolbox.**

Table 6 illustrates what may be communicated in terms of inputs and outputs at the various stages of the Risk Management Process.

**Table 6 – Inputs and Outputs of Risk Management Process**

<table>
<thead>
<tr>
<th>Inputs</th>
<th>Outputs</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Identification</td>
<td>Risk Identification</td>
</tr>
<tr>
<td>• Process steps</td>
<td>• Hazards</td>
</tr>
<tr>
<td>• Hard / Soft Data</td>
<td>• Risks</td>
</tr>
<tr>
<td>• Assumptions*</td>
<td>• Process Map</td>
</tr>
<tr>
<td>• Scope</td>
<td>• Assumptions*</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Risk Analysis</td>
</tr>
<tr>
<td>• Choice of Analysis Tool</td>
<td>• Risk Analysis Scores</td>
</tr>
<tr>
<td>• Rationale</td>
<td>• High Risks requiring immediate action / escalation</td>
</tr>
<tr>
<td>• Hard / Soft Data</td>
<td>• Assumptions*</td>
</tr>
<tr>
<td>• Assumptions*</td>
<td>• Scope</td>
</tr>
<tr>
<td>• Scope</td>
<td>Risk Evaluation</td>
</tr>
<tr>
<td>Risk Evaluation</td>
<td>• Tolerable Risk Level</td>
</tr>
<tr>
<td>• Rationale</td>
<td>• Rationale</td>
</tr>
<tr>
<td>• Assumptions*</td>
<td>• Assumptions*</td>
</tr>
<tr>
<td>Risk Reduction / Risk Acceptance</td>
<td>Risk Reduction / Risk Acceptance</td>
</tr>
<tr>
<td>• Resources</td>
<td>• Resources</td>
</tr>
<tr>
<td>• Processes for control</td>
<td>• Processes for control</td>
</tr>
<tr>
<td>• Capabilities</td>
<td>• Capabilities</td>
</tr>
<tr>
<td>• Decisions</td>
<td>• Decisions</td>
</tr>
<tr>
<td>• Actions</td>
<td>• Actions</td>
</tr>
<tr>
<td>• Assumptions* / rationale</td>
<td>• Assumptions* / rationale</td>
</tr>
<tr>
<td>Risk Review</td>
<td>Risk Review</td>
</tr>
<tr>
<td>• New hazards / risks</td>
<td>• New hazards / risks</td>
</tr>
<tr>
<td>• New data</td>
<td>• New action</td>
</tr>
<tr>
<td>• Changes</td>
<td>• Changes</td>
</tr>
</tbody>
</table>

*Note: Assumptions are made when little or no data is available at that time. This must be used with extreme caution as it could impact on the Risk Management process if they are found to be incorrect. Always aim to replace any assumptions at the next iteration of Risk Management or when information becomes available.

The level of detail communicated should be commensurate with the intended stakeholder’s needs and expectations. Enough information should be provided to allow for informed decision or assessment. Be aware that both too much or too little information can be counter-productive. For example:
A Guide to Supply Chain Risk Management for Suppliers to the Pharmaceutical, Medical Device and Allied Industries

- Senior Management usually do not require a detailed history, rather a concise summary of the situation with outputs of analysis and any decisions required;
- those preparing the summary will need detailed information / technical detail to base the analysis and recommendations on;
- recipients of the decision may just require a brief / letter outlining the decision and guidance for future action;
- the provider of the original information may require feedback that appropriate action has occurred.

When?

Communication activity must take place throughout the risk management process whenever appropriate to do so. Fundamentally these activities will occur at the beginning and end of each Risk Management stage. Communication is required when the following situations arise:

- unexpected developments – where urgent issues, occurrences or information comes to light, e.g. overdue information – this may replace previous information / assumptions and initiate a review of previously completed risk management stages;
- routine developments – as per the project plan or in accordance with the defined process within the scope of the risk management process;
- as per the needs of the stakeholders;
- at set project milestones such as the point of risk evaluation, risk control, risk acceptance, risk review and so on.

How?

The method of risk communication should be clearly established at each stage in the Risk Management process. Key decisions should be communicated formally. Elsewhere less formal methods will be sufficient.

When there is increased risk it is important to respond quickly so that relevant stakeholders receive accurate and timely information to make decisions and / or take action.

Always agree on the means of communication up front. The method of communication should be based on capabilities between parties. There is no point in expecting to communicate solely via e-mail if one of the parties doesn’t have a reliable electronic mail system or is unable to access one.

In Summary

- ensure the correct audience is identified;
- ensure the communication is suitable for the audience – concise, clear and traceable to all parties;
- communication should be timely for the intended audience or stakeholder;
- ensure through feedback that communication has been received and understood;
- ensure records are maintained;
- the methods and records should be able to withstand external scrutiny through appropriate and relevant documentary evidence.

[LINK to Toolbox Communication]

[LINK to examples]
1.8 Risk Review

Purpose

Risk Review is required to ensure that the outputs / results of the Risk Management process are periodically revisited and actively evaluated in response to events / new information. Change is constant albeit highly variable, and risks models can therefore be highly dynamic. Risk Review is about being able to demonstrate and verify the status and effectiveness of the Risk Management. It is sometimes referred to as “a sanity check”.

Without a planned review, the risk process will become gradually more out of date and cease to be valid. As a result new risks and variables will not be identified and assumptions will not be validated or moderated. This is wasteful of resources that have been invested in the original assessment.

Input

Risk Review can only begin once Risk Assessment and Risk Control has been completed. It requires the following information as a minimum:

- the results of original / previous assessment;
- any assumptions taken;
- monitoring information (planned feedback);
- any events or changes that have taken place since the previous assessment; and
- an interdisciplinary team.

Process

This section gives guidance on when, why and how to review the risk model, and the scope of the review. A review should enable the targeting of resource to areas based on assumptions, or new information that has come to light. It is not necessary to repeat the whole process with already identified and unchanged risks. The review requires that accurate information be reviewed and presented to the decision-makers.

A well executed Risk Review establishes that:

- the unknowns are minimised;
- new variables are identified and assessed and;
- the supply chain is controlled effectively.

Risk Management is a dynamic lifecycle. Review criteria are required at the outset of the process to ensure that it is updated periodically. Appropriate measurement tools should be established to monitor performance and feedback on any given process. Such information should be communicated to provide feedback to users and decision-makers to enable effective Risk Review.

An effective Risk Review process should accommodate the ability to respond to both Proactive and Reactive events:

1. Proactive  It is recommended that reviews initially be performed at least annually. Further reviews are dependant on the nature of the business (supplier history, known risks, assumptions and criticality of the product and processes).

Some examples of measurements:

- the actual performance of a new supplier against expectations;
- the outcome of a corrective / preventative action plan (CAPA);
2. Reactive Event triggers: New information or events can change the results of a Risk Assessment or at least indicate that a review should be performed (this is not an exhaustive list):

- new site for an established supplier (changes in operations, culture, capabilities and setup issues) or new product or service at an established supplier;
- technical changes in product or service supplied e.g. specification or a high rate of change;
- changes in markets supplied and in volumes produced;
- serious complaint / adverse event and or recall
- regulatory actions or incidents, such as Warning Letters, Consent Decrees or other unexpected events;
- changes in legislation (may be unforeseen);
- failure of supplier processes impacting quality and supply (e.g. deviations, complaints etc);
- results of audits or other visits;
- resources - (financial, personnel or equipment changes);
- new or modifications to monitoring systems;
- other significant issues impacting information used as a basis for assessment.

Some brief and illustrative examples of Reactive events:

- A distribution service supplier originally rated as very low risk reports their main warehouse in France has been partially destroyed by fire destroying 500,000 euros of finished product and affecting the status of 5 million euros of stock on the site. Was this:
  - a one-off low probability event as an accepted risk or an unforeseen event?
  - were systems mitigating this risk or other possible unrelated risk scenarios?
  - are other warehouses / markets at risk?
- A number of complaints are reported for an eye-drop finished product. Upon investigation a broker is identified in the supply chain and the herbal extracted ingredient has a different crystalline structure than original causing an adverse reaction. Events have since demonstrated the original assessment was based on inaccurate information and false assumptions.
- A key member of staff at a contract manufacturer leaves and the communication lines, flow of information and ability to interact between organisations breaks down..
- A Product Review highlights an unexpected series of deviations, or a trend relating to a service or material supplied.

The level of significance of an event trigger should determine if a review is required. Risks and risk indicators can change with time and with the change some risks require revaluation.

Some key questions to ask:

- has the probability of occurrence changed?
- has the impact or significance of known risks changed?
- are there any new areas to include in the Risk Assessment that has not been captured before?
are there any risk indicators that are no longer applicable due to changes in processes, equipment, suppliers, services, materials, circumstances etc.?

are there any new risk indicators or risk tools that should be used (process improvement)?

As well as having good communication and regular feedback relating to Risk Review, a process should be defined for the escalation of urgent matters to key stakeholders and decision makers including criteria and timescale.

[LINK – Risk Communication]

Output

The output / results of the Risk Management process should be reviewed to take into account new knowledge and experience. The outcome of Risk Review is not the end of the process. It is an iterative process that has a number of different outcomes:

- no action is required at present as all risks are known and under control, next review should be determined based on risk (about one year) or where new information / changes are made;
- new risks identified or assumptions are shown to be invalid requiring reassessment;
- a significant event, improvements or major gaps are identified that invalidate the original assessment resulting in a new risk assessment for that supplier or product.

Risk Review should be formally documented, approved and communicated.

In summary

Risk Management is an ongoing cyclical process, and not a one-off activity. It should enable control or eliminate large risks as well as identify any new risks and processes. The process should continue to be used for events that might impact on the original Risk Assessment decisions, whether planned or unplanned. As experience with the Risk Management process used grows, more advanced tools and methods may be used.
PART 2 – Risk Management Toolbox
PART 3 - Examples

This is a place marker for Parts 2 & 3 which will be incorporated within the final deliverable as the document would be too large to circulate for comment
## Annex 1 – Examples of Supply Categories & Requirements that reduce the Risk for Pharmaceutical Manufacturers

<table>
<thead>
<tr>
<th>Supply Category</th>
<th>Example of Requirements</th>
</tr>
</thead>
</table>
| Manufacturers of active pharmaceutical ingredients, excipients & raw materials | Adequate product testing performed to confirm compliance with customer and pharmacopeial specifications  
Cross contamination control precautions in place e.g. use of dedicated manufacturing equipment or effective cleaning verification of non-dedicated equipment  
Full traceability of raw materials including processing aids used in manufacturing processes e.g. animal derived, non-animal derived |
| Manufacturers of product contact consumables                                    | Appropriate materials of construction for product contact component (e.g. pharmacopeial recognised plastic or food grade)  
Full traceability of raw materials including processing aids used in manufacturing processes e.g. animal derived, non-animal derived  
Free from chemical and microbial contamination and easily to clean / sterilise |
| Manufacturers of product contact equipment                                     | Legible & fully completed documentation covering factory acceptance testing, calibration certificates & material conformity certificates  
Appropriate materials of construction used for product contact surfaces (e.g. 316L stainless steel, pharmacopeial recognised plastic) that are easy to clean and sterilise  
Minimal particle generation produced by moving parts (e.g. pumps) |
| Software designers / manufacturers                                             | Thoroughly completed and legible documentation with traceability of software changes from initial development to master copy  
Availability of master copy of software for back up purposes  
Knowledge of Good Automated Practice Guidelines (GAMP) |
| Manufacturing contractors                                                     | Effective quality documentation system compliant with required regulatory standard e.g. EU Guide to GMP  
Quality / technical agreement in place to define roles & responsibilities of each party.  
Effective contamination control measures in manufacturing facility e.g. environmental monitoring and product change-over procedures |
| Laboratory / Analytical Testing contractors                                    | Quality / technical agreement in place to define roles & responsibilities of either party.  
Full traceability of customer samples  
Testing performed to customer and pharmacopeial specifications and if necessary according to an effective out-of-specification results reporting procedure |
| Packaging contractors                                                         | Quality / technical agreement in place to define roles & responsibilities of each party  
Effective mechanisms in place for customer approval of labels and prevention of mix-ups  
Planned preventative maintenance and calibration of automated packaging lines |
| Wholesalers & Distributors                                                     | Approved, contractual agreement with customer  
Essential stocktaking, security, pest and segregation controls at storage facility with effective housekeeping, temperature control and |
<table>
<thead>
<tr>
<th>Supply Category</th>
<th>Example of Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>monitoring of storage area</td>
<td>Reliable transit temperature control &amp; full traceability of customer’s product</td>
</tr>
</tbody>
</table>
| Service providers (e.g. calibration, utility, pest control, cleaning etc) | Approved, contractual agreement with customer  
Specification of work and controls  
Reliable service with traceability of materials and instruments used to reference standards |
| Consultants                                 | Full curriculum vitae available for review  
Approved contract to define scope of work  
Evidence of experience and expertise required for customer’s project. |

Note: All suppliers should have an effective quality management system in place that is, where appropriate, certified to ISO 9001:2000.
# Annex 2 – Glossary (under development)

<table>
<thead>
<tr>
<th>Term</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Management System</td>
<td>The set of interrelated elements that establish policy, processes, procedures and objectives which direct and control an organisation with regard to all management activities.</td>
</tr>
<tr>
<td>Quality Management System</td>
<td>Quality Management System is a subset of interrelated elements that establish policy, processes, procedures and objectives which direct and control an organisation with regard to quality.</td>
</tr>
<tr>
<td>CAPA</td>
<td>Corrective and Preventive Action:</td>
</tr>
<tr>
<td>Hazard</td>
<td>A potential source of harm.</td>
</tr>
<tr>
<td>On Time in Full (OTIF)</td>
<td></td>
</tr>
<tr>
<td>Risk</td>
<td>The combination of the probability of the occurrence of harm and the severity of that harm.</td>
</tr>
<tr>
<td>Risk Acceptance</td>
<td>The decision to accept a quantified or qualitative amount of risk.</td>
</tr>
<tr>
<td>Risk Analysis</td>
<td>Estimation of the amount and severity of an identified risk using a tool such as risk ranking.</td>
</tr>
<tr>
<td>Risk Assessment</td>
<td>A systematic process of organising information to support a decision made within a risk management process.</td>
</tr>
<tr>
<td>Risk Assessment Tool</td>
<td>A recognised technique for the identification, prioritisation and management of key risks for example, Failure Mode Effects Analysis (FMEA), Fault Tree Analysis (FTA) and Risk Ranking and Filtering.</td>
</tr>
<tr>
<td>Risk Communication</td>
<td>Sharing the information about the accepted amount of risk to stakeholders.</td>
</tr>
<tr>
<td>Risk Control</td>
<td>Actions taken to accommodate a decision about a risk.</td>
</tr>
<tr>
<td>Risk Evaluation</td>
<td>Expression of a risk as a quantitative or qualitative estimation e.g. 1, 2, 3 or High, Medium or Low.</td>
</tr>
<tr>
<td>Risk Identification</td>
<td>Identification of the potential hazards and assessing the risks that those hazards pose. Risk identification addresses the “What might go wrong?” question.</td>
</tr>
<tr>
<td>Risk Management</td>
<td>The systematic process of assessing, controlling, communicating and reviewing risk.</td>
</tr>
<tr>
<td>Risk Reduction</td>
<td>Actions taken to reduce the probability or severity of the harm associated with an identified risk.</td>
</tr>
<tr>
<td>Risk Review</td>
<td>The mechanism used to constantly monitor events and improve a risk management process.</td>
</tr>
<tr>
<td>Risk Score</td>
<td></td>
</tr>
<tr>
<td>Term</td>
<td>Definition</td>
</tr>
<tr>
<td>------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Supplier</td>
<td>includes all suppliers throughout the supply chain that are important to</td>
</tr>
<tr>
<td></td>
<td>the user’s organisation based on risk including:</td>
</tr>
<tr>
<td></td>
<td>• Products (materials, components etc.);</td>
</tr>
<tr>
<td></td>
<td>• Services (e.g. calibration, cleaning, pest control, freight);</td>
</tr>
<tr>
<td></td>
<td>• Contractors (manufacturers, packing, warehouse, distributors, agents etc.).</td>
</tr>
</tbody>
</table>

| Supply chain |                          |
### Annex 3 – References and Bibliography (to be completed)

<p>| | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>1.</td>
<td></td>
</tr>
<tr>
<td>2.</td>
<td></td>
</tr>
<tr>
<td>3.</td>
<td></td>
</tr>
<tr>
<td>4.</td>
<td></td>
</tr>
<tr>
<td>5.</td>
<td></td>
</tr>
<tr>
<td>6.</td>
<td></td>
</tr>
<tr>
<td>7.</td>
<td></td>
</tr>
</tbody>
</table>