Rx-360 White Paper:

Managing Critical Vendors

Rx-360 Supplier Led Working Group

Lead Authors:

Rick Calabrese

Robin Kumoluyi

Wail Odeh

RX-360 WHITE PAPER: MANAGING CRITICAL VENDORS

Contents

Abstract and Introduction

Purpose

The manufacture of medical products, drugs and devices is highly regulated all over the world. All aspects of the manufacturing process, from product design to product delivery, require documented procedures. Key points in the process also require quality oversight and where needed testing. Risk assessment to determine the critical areas of the process is now mandatory for regulated companies and is required for non-regulated companies that follow the ISO 9001 quality management system starting in 2015.

One very important part of the whole manufacturing process is the proper sourcing and management of vendors that provide goods and services to the regulated company. This is one area in which it is very important to assess risk in order to properly manage production.

Every company should develop a program to assess and evaluate risk to determine the most critical vendors of their manufacturing process. Regulated companies have additional considerations when evaluating critical vendors. Such a program should focus on factors that can potentially disrupt the supply chain such as single source, regulatory compliance, unique capabilities of the vendor, and limited sub-tier suppliers to a key supplier. Both proactive and reactive monitoring should be utilized when managing critical vendors.

While a risk assessment or risk evaluation can be used as a tool to develop a plan to address potential issues, no plan is 100% perfect and sometimes unforeseen problems occur. When issues arise that affect a critical vendor, an action plan needs to be developed to mitigate the situation and prevent a disruption to the supply chain. This is especially true if the cause of the issue is related to regulatory compliance.

This paper will cover the key aspects of how to handle the management of a critical vendor that is under scrutiny and how to minimize the impact on the supply chain.

Scope

This paper will cover critical vendors that supply manufacturers (customers) of regulated products. The focus will be limited to first tier vendors. The process and best practices discussed are focused on regulatory areas of scrutiny but are able to be applied to other areas of quality concern.

Identifying and Defining Critical Vendors

Regulated industry (i.e. medical products, drugs and devices) is one that relies heavily on suppliers for the provision of materials (e.g. APIs, packaging components, excipients, etc.) and/or services (e.g. sterilization, testing, warehousing/distribution, etc.) to support their core business. Failures to meet the regulatory and compliance regulations requirements would potentially have a serious impact on the reputation and financials of an organization. The extent of the impact associated with supplier non-compliance varies and will depend on how critical the supplier is to the organization. Having a well-defined process for identifying and monitoring critical vendors is key to mitigating such risk. The following provides a summary of criteria to distinguish a critical supplier, recognizing that the distinction should be applied specifically and customers should be wary of identifying broad categories of suppliers as critical (e.g. although certain API suppliers may be critical vendors, not all API suppliers should automatically be considered critical.)

Over the years, supplier selection criteria have evolved and will continue to change as a result of increased competition, globalization of markets and changes to the regulatory landscape. Identifying critical vendors should be an integral part of the supplier qualification process. Factors that can be used to identify critical vendors may include, but are not limited to, the following:

1. Criticality of the materials and/or services to the business. Materials and/or services associated with the production of drug product and/or medical device that are i) medically necessary (lifesaving) and ii) have limited alternatives, should be considered critical.
2. Availability of the material and/or service. Material and /or services that are provided by limited number of suppliers or by a sole supplier pose a higher risk to business
3. Number of products/material supplied. The higher the number and/or volumes of material sourced from a supplier, the greater the risk to the supply chain.
4. Financial impact. This factor can be measured by how significant the disruption of supply of critical material and/or services by a supplier would be.

Considering the above listed factors, a critical vendor can be defined as:

- *A vendor that is deemed to be the major or sole provider of a critical materials and/or services, whose failure to supply goods/and or services would have the most significant impact on the organization/business.*

A vendor's criticality should be reevaluated on a regular basis as the criteria under which they are being evaluated are not static. For instance, a supplier deemed not critical during the initial assessment may be re-classified as a critical if they begin to supply new and more critical products and/or services.

Identification of Critical vendors will ensure that i) the critical vendors are subjected to the appropriate control and monitoring levels and ii) improve the utilization of available control and monitoring resources by assuring they are assigned where they are most needed.

Proactive Evaluation of Critical Vendors

Due Diligence & Audits

When evaluating a critical vendor, a customer should perform a comprehensive due diligence assessment. Having a well-defined due diligence process will allow the customer to compile documented evidence of the critical vendor's financial, technical, and supply chain capabilities. A best practice for a thorough due diligence process is to establish a detailed due diligence check list. Such a list will not only ensure that all aspects of the due diligence are being considered, but also expedite the process. The checklist can at minimum include, but should not be limited to, the following items:

1. General Project Information (.e.g. material/service to be provided, timelines, supply chain capacity, etc.)
2. Quality Systems where applicable (e.g., Quality policies and procedures, regulatory inspection history, quality unit roles and responsibilities and reporting structure, material management and control, facility and equipment, production control, etc.) along with quality culture.
3. Technical capabilities and capacity.
4. Tour of the supplier's site/facility (e.g. production area, quality control unit, facilities, etc.)
5. Environment, Health & Safety (e.g. EH & S policy and procedures).
6. Regulatory & Financials (e.g. regulatory filing abilities where applicable, supplier's financial performance history, cost of the service/material to be provided, etc.)

Depending on the criticality of the vendor, a due diligence team should include cross functional members. Representatives from Procurement, Technology, and the Quality Unit should always be part of the due diligence team. Regulatory, Engineering, Environmental, and Health and Safety may also be included as deemed necessary. Each member of the due diligence team should document the collected information and provide recommendations and/or action proposals related to his/her area of expertise. A detailed report of the due diligence assessment combining all the information should be prepared and final recommendation(s) presented to the Organization's Senior Management.

Due diligence is an imperative step of the supplier qualification process by which supplier's suitability can be evaluated.

KPIs and Trend Monitoring

Having a reliable critical vendor that ensures product and/or service availability where and when needed is very important for regulated industries. Key Performance Indicators (KPIs) are essential for the performance measurement process and are valuable for both the critical vendor and customer. KPIs help to identify and measure the levels of quality and/or service performance of a critical vendor. Implementing KPIs for critical vendors is key to identifying good practices, areas for improvement, and any trends which, if not addressed, may lead to supply chain disruption. KPIs should be measured from both customer and critical vendor's point of effort. The quality agreement between the parties should establish a process to manage and correct any discrepancies.

KPIs should include quality leading indicators that will provide some degree of predictability for potential future concerns and provide transparency on criteria for which the supplier will be evaluated. Agreed upon definition for each KPI must be established to ensure that it is collected consistently and that it supports its intended purpose. Customers should work jointly with the critical vendor upfront to establish KPIs, definitions, and quality indicators.

The quality KPIs used are dependent on the type of product or service provided by the supplier and the business relationship with the end user. Not all KPIs can be used in every case so it is important that the KPIs selected are discussed and agreed upon by both the supplier and the end user. Quality KPIs as discussed with the critical vendor related to the products/service provided may include but are not limited to the following:

1. Product/service rejection rate.
2. Customer complaint trends and/or rate.
3. Outcome of regulatory inspection, internal and client audits.
4. Deviations/non-conformances rate.
5. Right first time: This can be measured by the total number of products produced/service provided with no critical deviations/non-conformance vs the total number of products produced/service provided.
6. Overall employee training compliance.
7. CAPA Closure Rates.
8. Change Control.

A process for regular review of KPIs with the critical vendor should also be established. The frequency of the review may be determined based on how critical the critical vendor is to the organization. In general, a quarterly review of the KPIs is recommended, but companies should adapt KPI frequency to the nature of the business and capability of the vendor to provide the information. A scorecard system may serve as a method for monitoring KPIs.

KPIs are an invaluable proactive tool that greatly contributes to the monitoring and performance review process of critical vendors. Effective KPIs will allow an organization to proactively address any arising potential concerns to minimize or eliminate the impact to the supply chain.

Regulatory Notice and Monitoring

It is very important to develop a process for monitoring potential regulatory issues that can arise for a customer's vendors, especially critical vendors. The development of a program to identify events of concern and notification process is beneficial in managing any regulatory issues of concern. This includes a full risk evaluation and a process for obtaining and monitoring regulatory information.

A. Identifying events of concern

It is important to identify potential areas of concern with a critical vendor before they occur. The risk assessment should be designed to determine the critical aspects of the manufacturing process related to products or services provided by vendors. These critical areas must be analyzed in relation to applicable regulations. Once this is done a plan can be established based on which areas should be monitored.

The key areas of concern include but are not limited to the following categories:

- Quality system issues
- Import export issues
- Regulatory compliance issues
- Product or service regulatory requirements
- Loss of manufacturing license or Certificates of non-conformance

B. Notification methods.

Once the areas of concern as well as potential types of risks are identified, then a process can be developed to obtain notice of changes to existing regulations. A company should develop both internal and external processes for monitoring regulations and receiving notice of applicable changes. If a company is a multi-site facility spread over different regions, an internal communication plan should be developed to distribute regulatory information from one location to another. This can be facilitated by setting up a special email mailbox for this purpose. The scope of notification might also include any quality issues or incidents not driven by or directly related to the risk of regulatory action.

Externally, there are many different options. The basic option is to run an internet search for the specific topic of concern to find information or establish a system to run the search on a routine basis. There are also many free, as well as paid, subscription newsletter type services which can provide regulatory updates as well as regulatory actions regarding the vendors of concern or any products or services they may offer. For example, some publicly available databases include: FDA warning letters and import alert letters; the EDQM Database; and the Inspection Certification Database (FDA).

Companies can look also into periodicals like the US Federal Register which lists proposed changes to the regulations as well as requests for input to these proposed changes. There are services that will do numerous regular searches for a company on targeted regulatory information specifically important to that company or product set.

C. Regulatory Monitoring

Once the areas of concern have been identified and the method of notification has been established a company must develop a method of monitoring, evaluating, and processing the information obtained. It is not enough to just collect information; for it to be useful to a company it must be used proactively.

A checklist can be used with key criteria for identifying whether the information is relevant to a particular company. This is important as it is not very efficient to try to evaluate every piece of information received as not all of it will pertain to the company.

Once the information is deemed important, it must be evaluated for impact on the company and the company's products or services. One way to do this is to develop a "Regulatory Information Review Group/Board". This group can be made up of different subject matter experts including, but not limited to, QA, Technology Services, Engineering, & Operations. The SME's will be able to provide good feedback as to whether the information obtained will be impactful and must be acted upon.

D. Vendor Monitoring

Once it has been established that there is a potential for a regulatory cause for concern or issue it is important to contact the critical vendor and discuss the concerns up-front. This allows customer and the critical vendor to develop a plan for dealing with any potential issues before they occur. Consider also establishing routine phone conferences to discuss the products or services provided. Also, a site visit may be appropriate to perform a GAP assessment to gauge the potential of the regulatory issue of concern occurring at the critical vendor.

The key point is to have a process in place to act on any pertinent information obtained so the company can take the appropriate action with its critical vendors if necessary. A proactive approach can save countless man-hours and resources compared to attempting to mitigate a problem that has already occurred with no remediation plan in place.

Identifying and Evaluating Non-Compliance Issue(s)

Identifying and evaluating non-conformance issues is a crucial part of critical vendor management. Discovery or identification of the non-conformance may take place through varied communication and review channels. Routine audit activities, health authority inspection, product defect investigations and complaints, and notification upon self-discovery of the critical vendor represent the most likely channels of discovery. Because non-conformances can be illuminated through various processes and channels it is important that appropriate communication and notification processes are in place between the customer and critical vendor. Criteria should be agreed between the critical vendor and the customer regarding the criteria for, respectively, a critical, major, or minor incident. The associated responsibilities for each party to carry out in the case an incident is discovered along with the time frame for notification should be documented in a quality agreement or other relevant contract. Upon notification of the event, immediate evaluation is required to determine if there is an acute regulatory and compliance impact along with the associated actions required. It is important to acquire as much summary information about the event as possible in order to make the initial assessment. The initial assessment should determine the criticality of the event based on potential impact on product quality, regulatory compliance and patient safety. The depth of the event and boundaries of investigation (e.g. other batches, products, systems, or facilities, etc.) along with the potential impact on validation or qualification status should be determined as much as is possible during this initial phase.

The full investigation of the event, evaluation, and product disposition must be initiated in parallel to the initial assessment or started shortly after. The full investigation should begin with an investigation plan. The plan should take into consideration all the information gathered at the time along with a historical evaluation to determine if the event or similar events have occurred. All evaluations must be fully documented in an investigation report. Traceability on actions and activities must be transparent. All investigations must be completed and closed out to support the product disposition. All corrective and preventative actions (CAPAs) associated with the investigation must be monitored for assurance of completion, effectiveness, and closure.

a. Discovery of Event

Once an event has been discovered, it should be reviewed to determine the criticality of the event and the reporting and communication of such an event.

i. Discovered by the Customer:

The customer should escalate and document discovery of the event in their internal escalation/ management review systems. All relevant information to make an assessment should be gathered. In the case of a critical incident the supplier should be notified within 24 hours and given the preliminary information and advised of the actions taken thus far (e.g., notification to a Health Authority for potential market action). In addition, an investigation plan should be set forth describing the support required of the supplier along with the timelines.

ii. Discovered by the Critical Vendor:

Once an event is discovered the critical vendor should evaluate to determine the criticality of the event and the extent of the event in terms of customer impact. It is crucial to determine if the event is systemic and if it involves multiple processes and customer. The critical vendor should notify the customers of discovery of the event within the timeline agreed with customer. This is particularly important in the case of the need to report the incident to a Health authority e.g., FDA Field Alert Reporting (FAR) or Biological Product Deviation Report (BPDR).

b. Event Investigation

Once the initial information has been gathered on the event, where practicable, an investigation plan should be agreed by the critical vendor and the customer before additional work continues in particular before any additional analytical work is conducted. The opportunity for the customer to provide input will depend upon the business relationship and/or associated IP rights. The focus of the investigation must be to get to the root cause in order to prevent recurrence. The investigation plan should include the following elements:

- Team members and Lead Investigator
- Key tasks with responsible person(s) and associated due dates
- Documentation to be reviewed and who is responsible for providing the information, including relevant records such as batch/lot/site records, lab data, process data, event records, etc.
- Consideration of root cause analysis tool(s) to be used
- Timelines, including mitigation and follow –up resolution

In addition, a review of the event should be performed in regard to regulatory compliance. This review should be performed to determine the points of non-compliance which may require follow-up activities in regard to agency reporting and regulatory file adjustment.

Risk Evaluation: Product Impact

Risk evaluations of product(s) potentially impacted by the non-conformance or issues of concern must be completed to determine overall product compliance, quality and safety status. An initial risk evaluation should be performed quickly to determine if the compliance risk has the potential to create a product safety or efficacy issue as these situations are reportable events and require immediate action in order to protect patient safety. The risk evaluation must include all products that could be impacted and must span an appropriate bracketing time period of production which includes both product currently within your control and product already in the market place. Any risk evaluation should be performed within the scope of customer's established internal SOPs. An impact evaluation should include all marketed products, including products remaining under the control of the customer.

There are multiple aspects that must be considered when performing a product impact evaluation based on the nature of the non- conformance. These factors include an evaluation from both a retrospective and prospective review. The following aspects should minimally be considered:

Non- Conformance Type	Description	General Concern(s)	Minimal Evaluation Items
cGMP Inspection with critical violation in GMP systems	Lack of sufficient controls in place to support production of product or service provided.	Release without meeting specifications or requirements.	• Identify chronology of failure and active products • Full testing; • Historical data trend analysis of products: analytical history; deviation history; complaint history; stability
Product contamination or Product mix-up	The product has a contamination with a known or unknown substance e.g., the supplier has notified the customer that excipient x which is supplied has been contaminated during	The product is adulterated with an unintended contaminant The impact on the safety and efficacy of the product is unknown	• Analytical result evaluation- amount of contaminant present in material/ product • Literature search on the substance if known for behavior and toxicity levels-

Non- Conformance Type	Description	General Concern(s)	Minimal Evaluation Items
	production with material Y	The material could interact with the product or the patient in unknown ways and could pose a health risk. Stability issues.	• Calculation of permissible daily dose based on ICH Q3C • Evaluation of product interaction with the substance • Stability study
Data Integrity Issues	Lack of assurance that the data records are accurate, complete, intact, and maintained within their original context including their relationship to other data records.	Data does not support release of product without meeting specification and requirements. Traceability failure; non-compliance with part 11. Inability to provide supporting documentation upon request of regulatory agency.	• *Test data:* For cause technical visit to review records. • *Unintentional Systems:* Final product testing accounts for minimum requirements? • Complaint history • Stability testing • Remediation and interim controls at site.
Registration	Unapproved deviations from registration requirements as filed with health authority.	Inadequate site for production/services Improper labeling/release leading to recall Release without meeting specifications and requirements	• History of change • Current issue evaluation and associated systems (ie. unregistered specification, look at fit for purpose change history, complaints) • Registration classifications review

Non- Conformance Type	Description	General Concern(s)	Minimal Evaluation Items
			• Validation/qualification status • Contract agreements

In addition, the risk evaluation must include the rationale for the continued use of a critical vendor under remediation. Current trends indicate that there are concerns over the continued use of a critical vendor where the remediation plan does not explicitly provide a supporting rationale. Be aware that there may be additional risks specific to individual business models that require independent evaluation.

Risk Mitigation and Control

Measures to control, reduce, and ultimately eliminate the non-compliance and the potential deleterious impact or liability caused by the non-compliance issue must be taken in order to assure product safety and to restore the situation to a state of compliance. The approach and actions taken will vary depending on the nature of the non-compliance issue identified and whether it is a systemic or isolated issue. In all cases, for controls and risk mitigation to be effective, the situation must be viewed holistically including short term and long term measures. This is of particular importance where the supplier is critical and the product is medically necessary. The method and actions to assure safety and restore compliance must be documented and are best detailed in a remediation or CAPA plan with appropriate timelines and responsibilities. The plan must be developed through collaboration between the customer and the supplier to assure it can be operationalized and effective. Additionally, some plans depending on the state of non-compliance must be shared with the Health Authorities for which the manufacture holds a marketing authorization.

Collaboration

Collaboration and information sharing is key for building a strong relationship with critical vendors. Open communication and transparency is especially important in response to an event (e.g. regulatory actions, noncompliance) that may potentially lead to short or long term disruption of supplies. Meeting face-to-face to discuss such critical issues is proven to be the most effective form of communication. When a face to face meeting is not a viable option; holding periodic meetings via tele/video-conferencing can be just as effective.

Sharing best practices and offering the services of subject matter experts is imperative as it ensures the appropriate remediation plan is put forward. In order to be most effective, such a plan needs to be specific, clearly identifies roles and responsibility and includes buy-in from all stake holders.

Since the goal is restore compliance and to prevent the recurrence of such a critical event, it is essential to promote open communication and track whether or not all actions set forth in the remediation plan have been acted upon. Continuous assessment should be an integral part of this process, as it may yield new insights into improving the remediation plan and making it even more effective.

Remediation Activities

The elements below represent actions that can be taken singularly or in tandem in order to remediate a non-compliance situation. This list is not exhaustive and the actions taken will vary depending on the specific scenario and business model. Before implementing such actions, companies should evaluate applicability and feasibility based on the category of material, Intellectual Property (IP) rights, and the business relationship.

1. Interim Controls
   Short term remediation to allow for continued release while long-term remediation controls are implemented to correct identified non-compliance.

2. "Person in Plant"
   Under some business relationships where the product or service provided is specific for one customer a "Person in Plant" strategy may be utilized. This strategy provides a high level of over sight and allows for the customer to be on site during production of material or product or service to ensure that all their required procedures are being carried out according to the agreed parameters. The customer on site usually performs the following activities, evaluation of production start –up for their product, evaluation of material records, evaluation of in process data, review of all deviations associated with the product, review and approval of all batch records and final release of the associated product. In addition, the person is on site for consultation in real time as issues arise.

3. Incoming Material Control
   Strengthening sampling and testing practices in response to regulatory event, particularly in terms of frequency (no skip lots) and/or number of samples taken.

4. Full Release (monograph) Testing
   This is normally the case where the customer had been receiving material on a reduced testing scheme and has determined that full testing is required in order to assure reliability. This strategy allows the customer to perform or have independently performed full testing of the material in question in addition to the suppliers full release testing. The additional testing is compared to assure that the results are reliable.

5. Documentation Plan
   Request to see full background documentation on product prior to release.

6. For Cause/Follow Up Audit.

Exit strategy

It is important for a customer to develop a contingency strategy in the event they are no longer able to continue the relationship with the critical vendor in question. In developing this strategy, consider the potential impacts on the business. In determining when to take this step, consider the level to which the supplier is ingrained in current operations, the overall timing for potential exit, overall supply levels, regulatory filing considerations, knowledge transfer, and the availability and qualification of an alternative supplier.

Follow-up and Verification (CAPA)

An important part of the overall remediation process is to manage the issue of concern through the vehicles used to identify key problems or non-conformances. All non-conformances must be acted upon by the critical vendor. This includes audit findings, both internal and external, deviations and any non-conformances discovered by a regulatory agency. All of these must go through well-defined investigation and Corrective & Preventive Action (CAPA) process.

The observations or findings made should be evaluated by risk evaluation as to the criticality of the critical vendor and the critical vendor's ability to provide the company with products or services that are compliant with current regulations. The evaluation should include the potential regulatory impact or actions that might come against the critical vendor which would impact their ability to operate.

All responses made by the critical vendor need to be evaluated for completeness, accuracy and effectiveness in resolving the issue of concern by the customer using the products or services from the critical vendor. The customer must respond in writing to the critical vendor indicating whether they agree or disagree with the actions proposed by the critical vendor as CAPAs. Any concerns regarding the actions proposed must include the reason and rationale for the concern. This should be presented in writing and backed up by a conference call.

If the parties involved cannot come to an agreement, the topic should be elevated according to each party's internal escalation process until a resolution is agreed and documented.

Once the parties both agree on the issues, the critical vendor can then perform their investigation and root cause analysis to create any required CAPA. The information must be shared in writing with the customer and it is strongly recommended that this be followed up with a phone conference to ensure goals and objectives are properly understood by all parties.

Time frames for implementation are an important aspect of this process and periodic updates as well as method of updates need to be developed. This is especially true if the items of concern have been determined to be critical or more than one major issue of concern is involved.

Expectations must also be set regarding actions that must be completed in order for an issue to be considered properly addressed and closed. Time limits must be set up and agreed upon by both parties. This includes the time frame to prepare for the CAPA implementation, the implementation itself and the time it will take the local quality group to verify the CAPA has been properly implemented and the timeline for performing their own internal CAPA verification to ensure that the CAPA is effective as per predefined requirements listed in the CAPA plan.

The follow up and verification of the CAPA plan by the customer should be strongly aligned with the activities of the critical vendor related to the CAPA program. At each of the predetermined CAPA plan milestones a notification should be sent out to the customer from the critical vendor detailing the disposition and outcome of that particular milestone. When appropriate, objective evidence should be sent to document the activities of the milestone. This can include, but is not limited to, pictures, standard operating procedures, maintenance/installation reports, and validation reports.

Routine phone meetings should also be set up at appropriate intervals to keep the customer well informed of the nest activities taking place.

Finally when the CAPA has been fully implemented and signed off as being effective by the critical vendor's quality team, the customer should perform an on-site audit and have their own quality auditors verify that the CAPA has been properly implemented and verify its effectiveness for the timeframe.

If there are critical regulatory issues of concern or several major regulatory issues of concern, a follow-up audit should be set up at a time frame after the CAPA verification Audit. All these actions need to be properly documented on an audit report and reported back to the management of the customer. After evaluation by the management team, which can include SME, the customer can then take appropriate operational actions as to the disposition of the status of that critical vendor.

Prevention Summary

“Prevention is better than cure.” Identifying critical vendors at the earlier stages of the supplier qualification process will ensure that they are subjected to appropriate controls and monitoring levels. The level of visibility to supplier operations is essential for an early detection of potential quality and compliance concerns. This visibility can be established by i) increasing the frequency of onsite audits or onsite technical visits and ii) agreed upon quality Key Performance Indictors (KPIs) which can be reviewed by all stake holders on a regular basis (e.g. monthly, quarterly, etc.). Such advance planning can serve end users well even when events cannot be prevented by creating clear and established processes for identifying issues of concern or non-compliance events, as well as placing protocols for risk assessments and product impact evaluations, mitigation, and vendor follow-up. The bottom line is that open and clear communication between all parties can go a long way to help prevent issues before they arise.