# Guidance Document for Implementation of Vendor Risk Management Grid

**Authored by:**
Critical Path Consultants, Inc.

Pleasanton, CA: 925.932.4325
(ncaserma@criticalpathconsultants.com)

**Vendor Risk Management Grid**
**Implementation Guidance**

**Introduction**
Structuring an effective vendor audit program begins with analysis. According to Steve Dunning, head of KEMA's Western Region ISO practice, "ISO 13485 requires you to have documented systems for vendor management where appropriate – but first you have to do some type of risk assessment to determine what's 'appropriate'".

However, simply positioning vendors along a linear scale (according to inherent product/service risk) ignores important, real-world business considerations: vendors who supply a high dollar value of products/services obviously merit more scrutiny than vendors who supply a lower dollar value of products/services. Thus, evaluating vendors according to "risk" versus "value" can help to determine relative audit priorities. The attached Vendor Risk Management Grid provides a framework for performing this analysis.

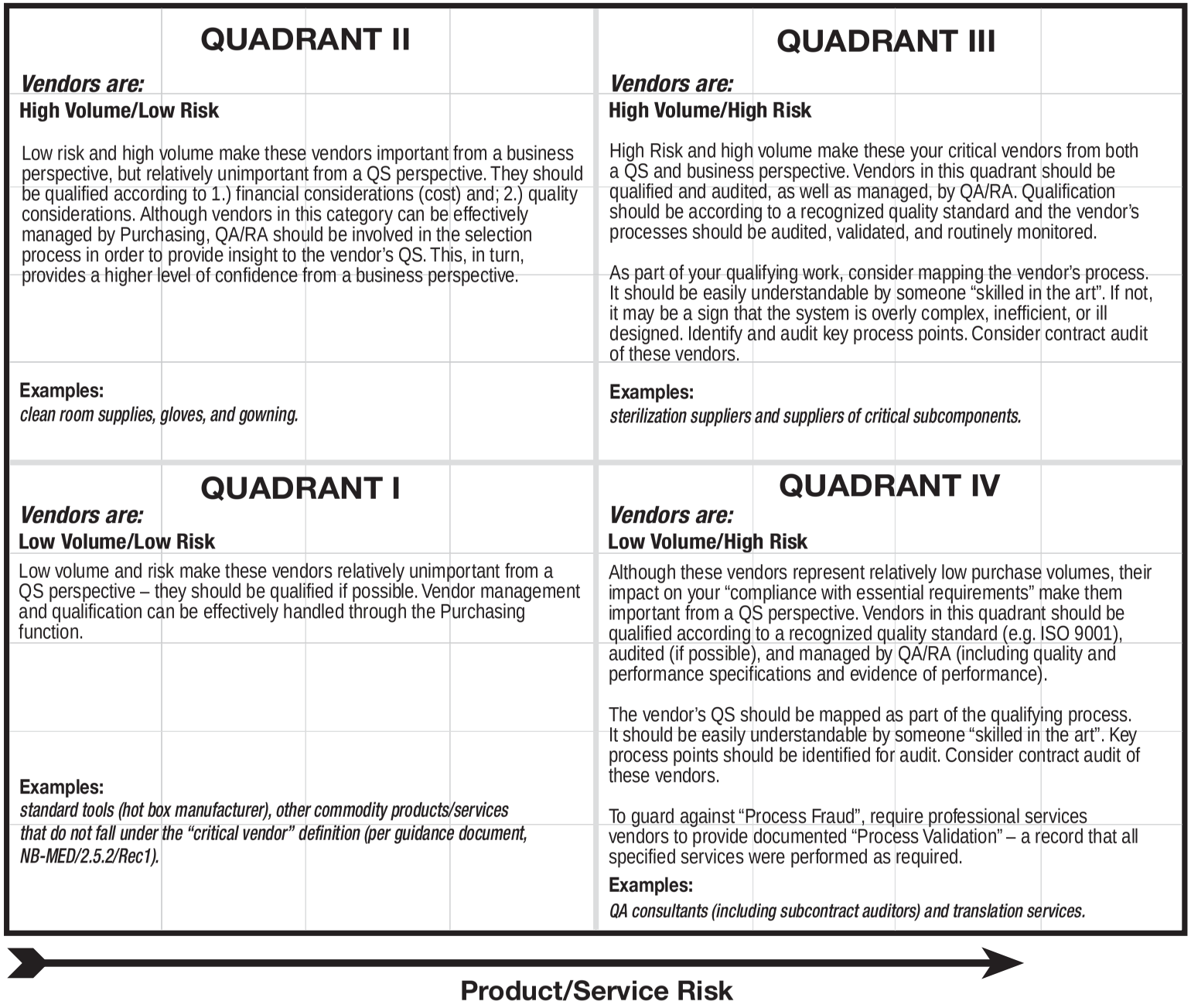
**Notified Body Guidance on "Critical Vendors" (also utilized by CMDCAS)**
Equally important, from a risk management perspective, is the determination of who is (and who is not) a critical vendor. Making this assessment enables you to accurately position vendors along the "*product/service risk*" axis of the Vendor Grid. Notified Body Recommendation **NB-MED/2.5.2/Rec1** ("*The manufacturer's responsibility for the quality of the subcontractor's performance of quality of their products*") provides important guidance in this regard. Specifically, the guidance document states (underlining and bracketed comments added to illustrate key items):

> *The two main issues a Notified Body should address when reviewing subcontractors are:*
>
> *a) Whether the subcontractor has a substantial involvement with the design and/or production of the device [i.e. outsourced manufacture].*
> *b) Whether the subcontractor is undertaking the supply of a part, material or service, which may affect the compliance of the device with the essential requirements [note that services which affect conformity are also included in this definition].*
>
> *If the answer to both a) and b) above is NO, no further action is required.*
> *If the answer to a) or b) above is YES, then the Notified Body must evaluate whether there is sufficient evidence provided of the competence of the subcontractor to undertake supply of the part, material or service in relation to the medical device(s) in question. The evaluation will consider various matters including the control exercised by the manufacturer over the subcontractor and the certification held by the subcontractor.*
>
> *In all other circumstances, the Notified Body must be allowed to review the relevance or criticality of the subcontractor to the medical device and, if not satisfied by the evidence available from the manufacturer, under-take an audit/assessment of the subcontractor or require the manufacturer to under-take a re-evaluation of the subcontractor.*

The final section regarding audit/assessment of subcontractors is especially important for manufacturers. In order to provide compelling evidence for Notified Bodies, the manufacturer should have 1.) A well-conceived rational for the critical/non-critical determination and; 2.) a well-prepared audit/assessment for critical subcontractors.

A well-prepared subcontractor audit/assessment can best be performed by an individual with process audit experience. ISO registrars such as KEMA recommend outsourcing subcontractor audits to individuals with industry-specific and process audit experience.

Following is an illustration of a Vendor Risk Management Grid with explanatory notes to help guide you in your analysis:


QUADRANT II
Vendors are:
High Volume/Low Risk
Low risk and high volume make these vendors important from a business perspective, but relatively unimportant from a QS perspective. They should be qualified according to 1.) financial considerations (cost) and; 2.) quality considerations. Although vendors in this category can be effectively managed by Purchasing, QA/RA should be involved in the selection process in order to provide insight to the vendor's QS. This, in turn, provides a higher level of confidence from a business perspective.
Examples:
clean room supplies, gloves, and gowning.
QUADRANT III
Vendors are:
High Volume/High Risk
High Risk and high volume make these your critical vendors from both a QS and business perspective. Vendors in this quadrant should be qualified and audited, as well as managed, by QA/RA. Qualification should be according to a recognized quality standard and the vendor's processes should be audited, validated, and routinely monitored.
As part of your qualifying work, consider mapping the vendor's process. It should be easily understandable by someone "skilled in the art". If not, it may be a sign that the system is overly complex, inefficient, or ill designed. Identify and audit key process points. Consider contract audit of these vendors.
Examples:
sterilization suppliers and suppliers of critical subcomponents.
QUADRANT I
Vendors are:
Low Volume/Low Risk
Low volume and risk make these vendors relatively unimportant from a QS perspective – they should be qualified if possible. Vendor management and qualification can be effectively handled through the Purchasing function.
Examples:
standard tools (hot box manufacturer), other commodity products/services that do not fall under the "critical vendor" definition (per guidance document, NB-MED/2.5.2/Rec1).
QUADRANT IV
Vendors are:
Low Volume/High Risk
Although these vendors represent relatively low purchase volumes, their impact on your "compliance with essential requirements" make them important from a QS perspective. Vendors in this quadrant should be qualified according to a recognized quality standard (e.g. ISO 9001), audited (if possible), and managed by QA/RA (including quality and performance specifications and evidence of performance).
The vendor's QS should be mapped as part of the qualifying process. It should be easily understandable by someone "skilled in the art". Key process points should be identified for audit. Consider contract audit of these vendors.
To guard against "Process Fraud", require professional services vendors to provide documented "Process Validation" – a record that all specified services were performed as required.
Examples:
QA consultants (including subcontract auditors) and translation services.
Purchase Volume
Product/Service Risk