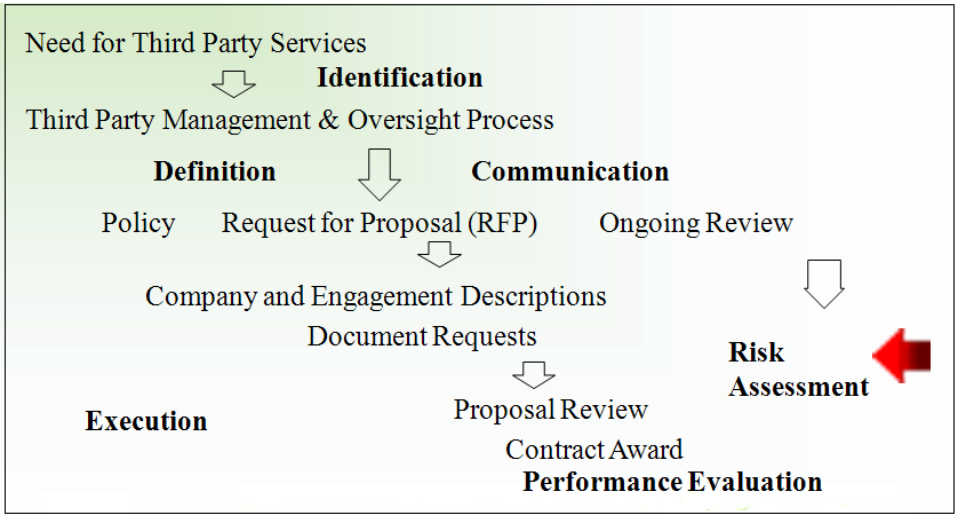
Corporate Vendor Management and Oversight Risk Assessment: Perception versus Reality

Ask any two people to describe a process and you are likely to get two different answers. Ask twenty people to comment on how well the process is working, and you will receive a still wider array of responses. Broaden the pool of participants to 200 or 2,000, and answers will fall along the spectrum of all possible reactions. How, exactly, does this fit into an auditor's world of objective criteria and black and white conclusions? And what benefit to management is this hodgepodge of data?

A case study in Vendor Management and Oversight risk assessment explains.

Vendor Management and Oversight (VMO) is not only a requirement, but an area of increased focus by the auditors and regulatory agencies across all disciplines. Companies are now outsourcing many of their functions to third parties and are expected to manage these relationships to ensure that all services are delivered to their customers according to a certain standard of expectations, and that confidential information is safeguarded against unauthorized access or use.

A typical VMO framework (pictured below) includes the components of identification, definition and communication, execution, and performance all within a defined set of parameters. A comprehensive risk assessment ensures that the foundation, deliverable and review are all sufficient enough to mitigate the exposure to loss of reputation, customers, or income.



The VMO process starts with the development and adoption of a Vendor Management and Oversight Policy, which defines the vendor classification criteria, Request for Proposal (RFP) process, selection of qualified vendors, contract for engagement, performance standards, and mutual nondisclosure and confidentiality agreements. In addition to setting the company's standards for VMO, the Policy is an excellent starting point for the internal auditor, and can be used for the basis of the risk assessment and audit plan.

The Request for Proposal (RFP) is a multi-part document that identifies the company and the project, outlines the proposal process, defines the schedule of events and related deadlines,

compels compliance with all laws, and provides the vendors with a list of items that must be provided for consideration for the project's contract award.

Contracts are awarded based on the review of the RFP responses. Once signed by authorized parties, the executed contract governs the expectations, services, and deliverable of the vendor. The contract will also contain a time frame within which it will be valid, the frequency with which the service will be performed, all applicable timetables and schedules, methods of data transmission, format of the final deliverable, an expected final deliverable or service cessation date, and the conditions for any modifications or cancellations. Confidentiality and mutual non-disclosure agreements should be part of the contract.

Vendor risk assessment is a continuous process initiated at the time of the vendor contact and sustained through the evaluation of the performance of services. While the auditors are generally tasked with this review, the effects of a good, or bad, vendor are felt institution-wide.

An effective vendor management and oversight risk assessment occurs when the process is evaluated from several perspectives. One of the tools employed is the audit plan, which normally utilizes narratives, flow charts, internal control questionnaires, and test steps, and is structured around a well-defined and focused scope.

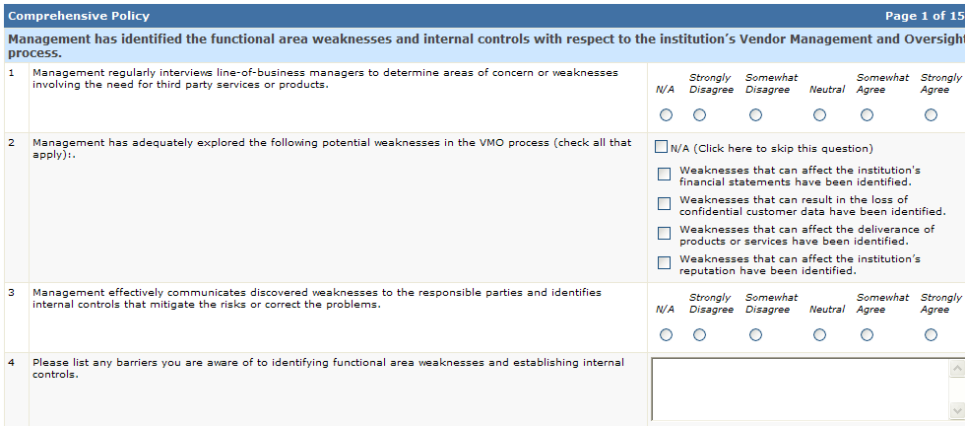
An assessment that recognizes the regulatory requirements, industry best practices, and the institution's geographical differences and functional insights is an excellent opportunity to identify both strengths and weaknesses in the program and the vendors.

Results are precipitated by answers to the various questions presented within the Risk Assessment survey. Questions are filtered by function, including organizational structure, title, job responsibility, employment status, and geographical location. Respondents only answer those questions that are relevant to their department or experience. Management and Audit/Compliance will be responsible for more questions than will other departments. It's also possible to allow Board members and/or vendors to participate in the survey. Drill down and slice-and-dice capabilities are possible using single or multiple demographic criteria for analytical review.

The survey statements should be answered honestly and in the spirit of helping the company assess its current situation. There are three types of questions:

Questions #1 and #3 below are examples of questions designed to gauge the level of understanding of the processes and procedures at the company. For each statement, the choices score the level of agreement or disagreement with that statement, scaling the answer on the 1 – 5 scale. The scale ranges from 1 (Strongly Disagree) to 5 (Strongly Agree).

Question #2 below is an example of a multiple choice question for which there are a number of alternatives that represent competencies, policies and practices of the company.



Comprehensive Policy Page 1 of 15

Management has identified the functional area weaknesses and internal controls with respect to the institution's Vendor Management and Oversight process.

1	Management regularly interviews line-of-business managers to determine areas of concern or weaknesses involving the need for third party services or products.	N/A · Strongly Disagree · Somewhat Disagree · Neutral · Somewhat Agree · Strongly Agree
2	Management has adequately explored the following potential weaknesses in the VMO process (check all that apply):.	☐ N/A (Click here to skip this question) ☐ Weaknesses that can affect the institution's financial statements have been identified. ☐ Weaknesses that can result in the loss of confidential customer data have been identified. ☐ Weaknesses that can affect the deliverance of products or services have been identified. ☐ Weaknesses that can affect the institution's reputation have been identified.
3	Management effectively communicates discovered weaknesses to the responsible parties and identifies internal controls that mitigate the risks or correct the problems.	N/A · Strongly Disagree · Somewhat Disagree · Neutral · Somewhat Agree · Strongly Agree
4	Please list any barriers you are aware of to identifying functional area weaknesses and establishing internal controls.	

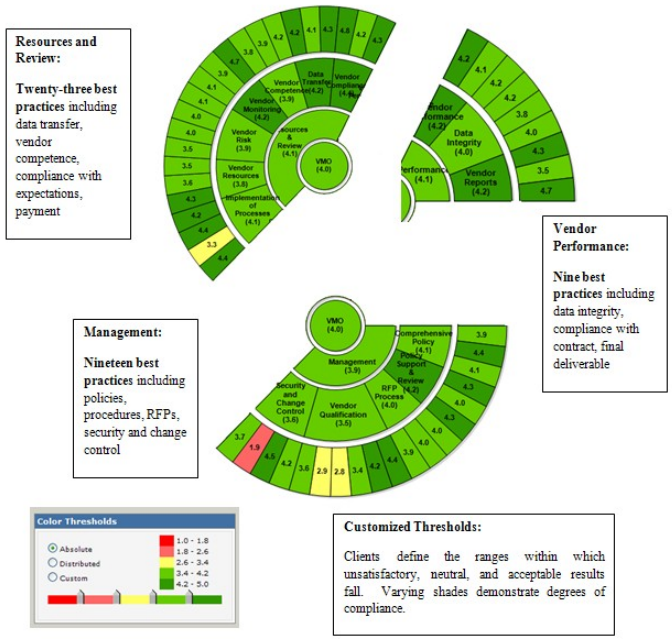
The Open-Ended questions, similar to #4, are an opportunity to point out specific problems, issues, or items of concern. These questions should be answered only when there is a clear issue to be addressed.

Summary charts allow for a quick review of the final survey results. In this particular assessment, the outermost ring represents 51 best practices.

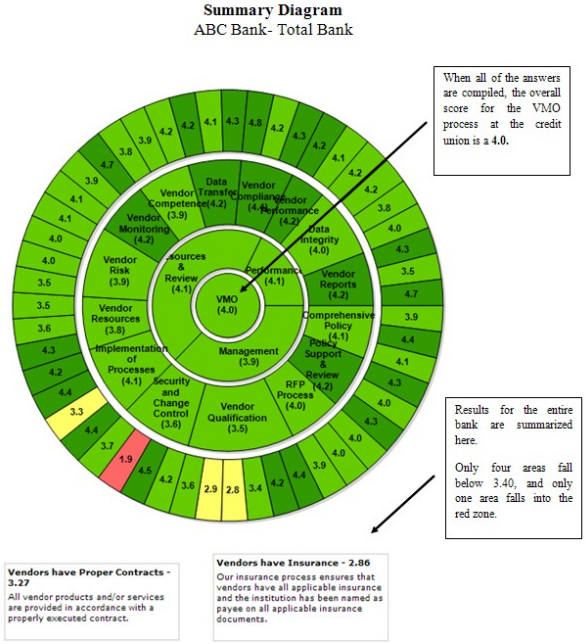
Rolling into those best practices are 155 individual questions that serve to assess the perceptions and realities of the current environment.

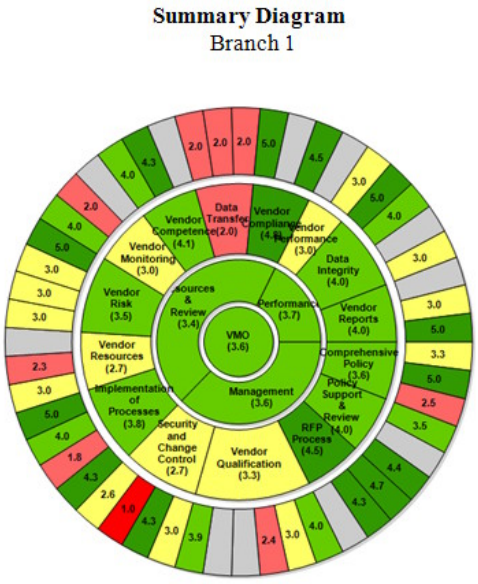
The best practices are then summarized into 15 functional categories, and then into the three main sections of Management Responsibilities, Execution and Performance, and Resources and Review. The innermost circle represents the summary total of all responses.

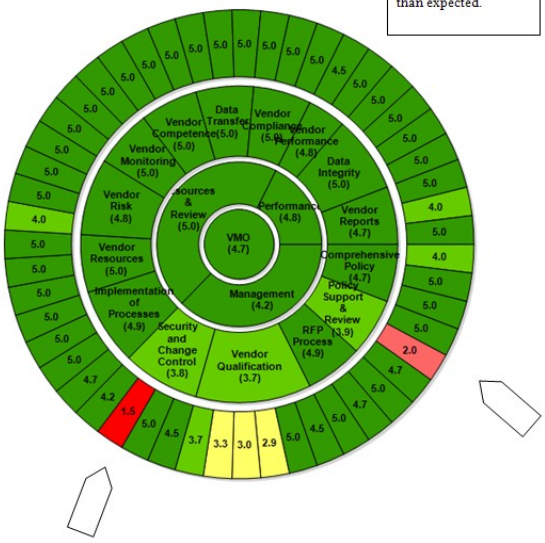
Responses can be reviewed by total company, branch, or function. Examples from a recent case study are presented for

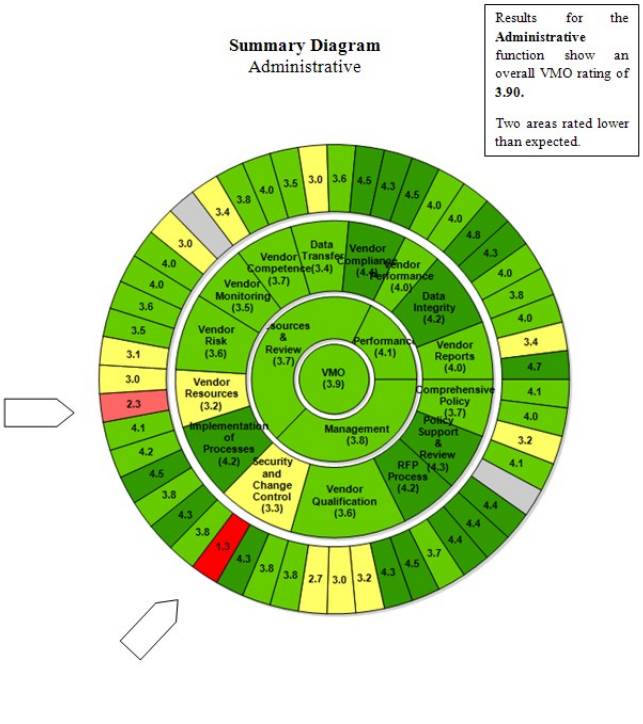


review. Compliance with guidelines and parameters can be objectively measured and quantified. Risks and responses should be weighted and assigned unique factors. For example, values of 1-5 can be assigned, with 5 being the most desirable rating. The answers should be evaluated in terms of strengths and weaknesses, opportunities for corrections and enhancements, and importance with respect to regulatory concerns, industry best practices, customer retention and cost. Answers should be presented by subcategory and compliance status. Green areas present little concern for risk, while those areas in red represent potential for exposure.

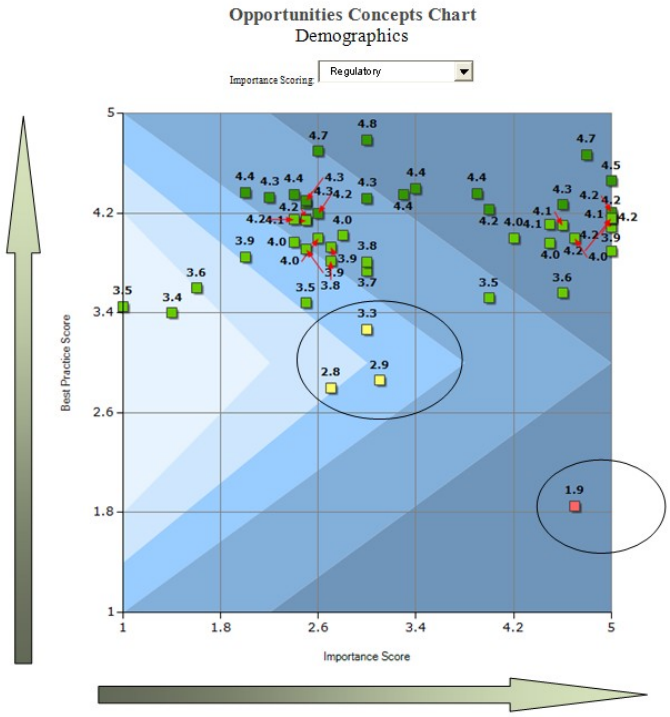








The Opportunities Concept charts plot the summarized answers on the Y axis and the goals on the X axis to enable management to most effectively deploy resources. Four goals are used: Regulatory requirements, best practices, customer retention and cost. Companies can use the matrices to determine where to most effectively deploy their resources.



The risk assessment was quite the eye-opener to the client. While management and the audit department were quite confident that the internal VMO process was sufficient to mitigate the risk of exposure via faulty processes or vendors, the internal perception was that the process was cumbersome, incomplete and often circumvented. A VMO audit performed in tandem to the risk assessment proved the assumption that the process was competent and met all regulatory standards. However, possible exposure did exist in terms of lack of communication and understanding internally.

In conclusion, vendor management and oversight is exposed to inherent risks in both the vendors and the process. However, a strong policy reinforces the requirements for vendor management and oversight and the RFP defines the documentation required for each project; the contracts specify the expectations of performance and safeguarding of data; the maintenance program continuously monitors the request and receipt of supporting vendor documentation and the audit program provides a systematic and objective methodology for risk assessment.

Deborah Donaldson is President and CEO of Alpha-Numeric Consulting, LLC, (www.alphanumericconsulting.com) a national consulting firm that specializes in audit program preparation, audit work, vendor management, risk management, asset liability management, profitability, and continuing education in related areas. She is a nationally known speaker and educator, and regularly participates in webinars, seminars, roundtables, and industry forums. She is also a published author of both fiction and nonfiction. Ms. Donaldson has more than 20 years of experience, with concentrations in audit (investments, loans, deposits, trust, branch operations, IT, etc), risk management, and profitability. She is currently serving as the Chair of the internal audit committee of the Financial Manager's Society, FMS Board member, editorial advisor to the Internal Auditor Alert newsletter and is a member of The Institute of Internal Auditors. Ms. Donaldson is the author of the Internal Audit Desk Reference Guide, 2nd Edition,

offered by FMS, and is co-authoring, for FMS, a book on the validation and verification of ALM models.