WHY Have a Vendor Management Process?

- To protect the Enterprise;
- To adhere to Regulations, if you are in an industry which requires a proper and controlled Vendor Management process; Examples: Financial Institutions; Pharmaceuticals; Insurance;
- To assist in monitoring, measuring, mitigating risk;
- To promote and encourage the best vendor(s) and overall quality.
HOW to commence the Vendor Management process

- Identify **ALL vendors**;
- **Rank or rate them**—low, medium, high;
- Create a separate list (spreadsheet) for vendors ranked “high;” Are the vendors publicly traded or privately held?
- Begin the annual “financial stability assessment;”
- Develop a Vendor Management Policy.
On-going Monitoring

• Assign personnel to review these high ranked vendors, as least quarterly. Review the vendors’ web sites, magazines, major newspapers, nightly news, etc., to see if any negative stories have impacted these vendors. Report concerns to senior management. Examples; fines; litigation; financial irregularities, etc.
Develop a comprehensive Vendor Management Policy

• Working with senior management, purchasing, business lines, compliance, IT, etc., write the policy, and submit it for BOD approval, if one if not in place. Update it annually.
Involve Audit!!

- Whether audit is outsourced or is performed by an employee, please communicate this process to audit, so they may add Vendor Management to the Audit schedule.
On-going process

- Review and update: the critical vendor list and the policy.

WHY?

- Organizations acquire new business lines, move locations, divest businesses, add new hardware or software, move to other countries, etc.

- All enhancements should involve senior management and BOD approvals.
Written Contracts!

• This process is known to all, but . . .
• Determine if there are written contracts between the enterprise & the vendors.
• Legal Department involvement is essential.
• Define your needs—customer service; how are software updates controlled?
• How are employees being trained to use the produce or service?
Written Contracts (cont’d)

• Obtain a list of references to determine customer satisfaction with the vendor, if this is a new vendor you are negotiating with;
• How are errors and corrections going to be addressed by the vendor?
• Price? Inflationary Increases?
• If the enterprise wants to end the contract, how much notice should be given? Fees?
Vendor Contracts (cont’d)

• Who is going to be responsible for information security—user access, passwords, encryption, follow-ups/investigations for security violations?

• If special enhancements are requested by the clients, what additional fees are assessed? Examples: additional reports, new screens, etc.

• Is the vendor measuring/monitoring customer satisfaction? How?
Vendor Contracts (cont’d)

• Back-up and Disaster Recovery—does the vendor have a written plan? Obtain this and review.

• Right to audit clause—determine WHO is going to audit these above-mentioned processes at the vendor?
Thank you!!

Contact: Diane C. Wilmanski, CISA and M.B.A.

DWilmanski@hotmail.com