Third-Party Risk Management Workbook

Myths

Vendor Pre-Assessment

Risk Profile Tiers

Inventory

Due Diligence Checklist

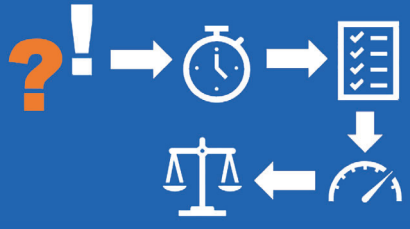
Risk Remediation Checklist

Risk Acceptance

Third Party Risk Management Process

Integration

HALOCK®



MYTHS

What is the truth?

“Our data is _____; it’s in AWS.”

“They’re _____, a SOC report was provided.”

“They have a _____ Information Security Program, we reviewed them a couple years ago.”

“They’re no longer a _____, we terminated the contract.”

“They had a breach, we are not _____.”

“Our business partners _____ know what vendors they use.”

Vendor Pre-Assessment

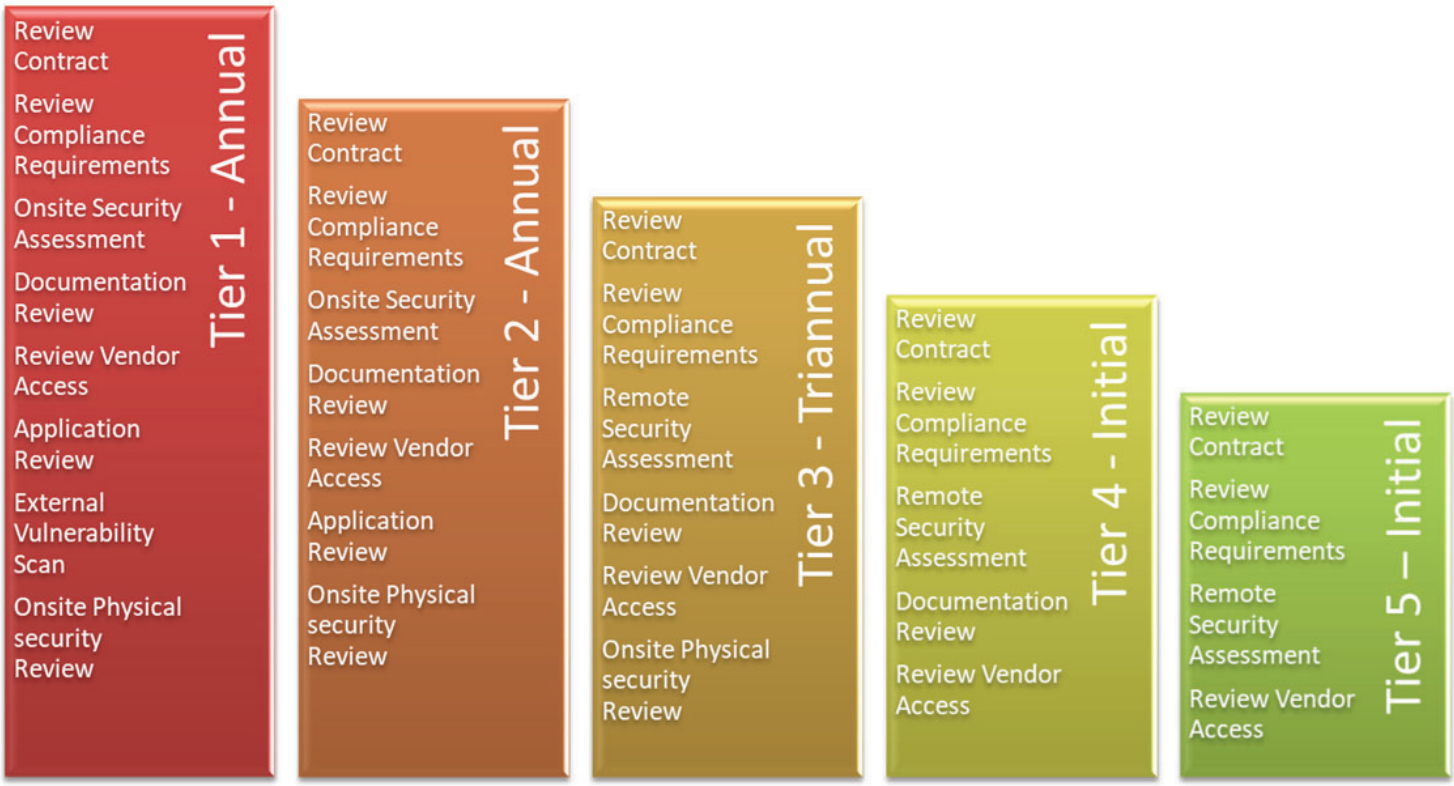
Vendor Pre-Assessment	
TO BE COMPLETED / VALIDATED BY REQUESTOR	
Business Partner Name	
Contract Number or Title	
Business Unit utilizing this Business Partner	
Executive Owner for this Business Relationship	
Vendor Contact Information i.e. POC, name, phone, email, etc.	
Vendor Locations Information	
Provide a detailed description of the services that the Business Partner will be providing.	
List the data elements that will be shared with the vendor?	
What is the volume of records sent and how often?	
Is the information shared with the vendor protected by legal, contractual and regulatory requirements i.e. PII, ePHI, or financial information?	
Have SLA agreements been defined; what are the acceptable downtime requirements?	
Does the vendor have external access to our network i.e. physical access, remote access, VPN, Site-to-Site, etc.?	
How is the data transferred to the vendor i.e. email, fax, SFTP, etc.?	
Does the vendor have access to the data at rest?	
What is the value of the contract and how long is the term?	

Inherent Risk Profile

Vendor:	Hyper Analytics		Inherent Risk:	High	
Date:	1/1/2019		Vendor Tier:	Tier 1	
Factor	**Low**	**Minimal**	**Moderate**	**Significant**	**High**
Type of information	No Data	Public information, non-regulated	Internal use only information (e.g., policies, procedures, routine memorandums)	Confidential information, intellectual property (trade secrets).	Regulated information (PII, NPI, PHI, cardholder data)
Volume of Information	1 – 100 of Records	100 – 1,000 of Records	1,000 – 10,000 of Records	10,000 – 500,000 of Records	500,000 + of Records
Legal and Regulatory Requirements	Not regulated legally or by contract	Statement of Work	Subject to contractual requirements mandating the exercise of due care	Subject to GLBA, SOX, GDPR, FACTA, etc.	Subject to PCI DSS, FFIEC, HIPAA
Criticality of Service to Business	No SLA (Service Level Agreement) requirements	Services can be unavailable for more than a month without materially disrupting "ACME"'s business	Services unavailability for one week to one month will materially disrupt "ACME"'s business	Services unavailability for less than a week will materially disrupt "ACME"'s business	Service unavailability for less than a day will materially disrupt "ACME"'s business
External Access	No External Access	Remote access session monitor by internal personnel	Vendor is issued a remote access client or web portal access	Site-to-site VPN tunnel; remote access client terminates on internal systems	Internal network/systems hosted on external vendors infrastructure
Data Transfer Services	No Data Transfer	Secure file transfer to Vendor	Secure file transfer from Vendor	Insecure file transfer to or from Vendor	Vendor has direct access to internal data
Access to Data at Rest	No access to data rest	Monitored Vendor access to internal data at rest	Vendor granted assess as needed to internal data at rest	Vendor has unmanaged authenticated access to internal data at rest	Data at rest on internal or external Vendor managed systems
Size of Commitment	Cost is less than $50,000, one-time	Cost is less than $50,000, one year term, impacts few "ACME" users	Cost between $50,000 and $100,000, two to three year term, impacts dozens of "ACME" users	Cost between $100,000 and $500,000, three to five year term, impacts dozens of "ACME" users	Cost greater than $500,000, greater than five year term, impacts hundreds of "ACME" users
Number of Statements Selected in each Risk					

Once a risk rating is selected for each risk factor, the overall inherent risk rating for the third party service provider is calculated taking into account multiple combination. Third Party risk manager will review the combination of risk factors and assign a given Vendor Tier, see Tab (Due Diligence Tiers)

Vendor Inherent Risk Tiers



Service Provider Inventory

Service Provider Inventory

Up For Review	Contract ID	Vendor Name	Service Type	Data Type	Inherent Risk	Vendor Tier	Last Review Date	Next Review Date
	HC0001	Aquifox	Credit Reporting	PCI, ePHI,Private	High	Tier 1	3/1/2018	3/1/2019
	HC0002	Liquid Hill	Shredding	Private	Low	Tier 3	1/1/2017	1/1/2019
	HC0003	T.T. Ronald	Logistics	Private	Moderate	Tier 2	10/1/2017	10/1/2019
	HC0004	Unitedtrans	Logistics	Private	Moderate	Tier 2	7/1/2017	7/1/2019
	HC0005	Hyber Analytics	Data Analytics	PCI, ePHI,Private	High	Tier 1	6/1/2018	6/1/2019
	HC0006	Data Theraby	Data Analytics	Private	Significant	Tier 1	1/1/2018	1/1/2019
	HC0007	Epic Image	Print/Image	Private	Minimal	Tier 3	1/1/2016	1/1/2019
	HC0008	SecureZipe	Data Cleansing	Private	Significant	Tier 1	7/1/2018	7/1/2019
	HC0009	Shred-dot	Shredding	Private, ePHI	Minimal	Tier 3	10/1/2016	10/1/2019
	HC0010	Speediezz	Shipping	Private	Low	Tier 3	1/1/2016	1/1/2019
	HC0011	UberData	Data Analytics	PCI	High	Tier 1	11/1/2018	11/1/2019
	HC0012	HydroList	Data Cleansing	Private	Minimal	Tier 3	1/1/2016	1/1/2019
	HC0025	AmzSure	Data Analytics	Private	Moderate	Tier 2	9/1/2017	9/1/2019

Due Diligence Checklist (Initial and Subsequent)

Item	Characteristics	Commentary / Observations	OK?
Legal Review	Contract Review: Y / N Compliance Review: Y / N		
Audit Report	SOC: 1 / 2 Type: I / II Auditor: _____ Test Period: ___/___ to ___/___ Opinion: Qualified / Unqualified Control Exceptions? Y / N		
Financial Statements and Credit Information	Issued: ___/___/___ Audited? Y / N Profitable? Y / N Excessive Debt? Y / N D&B Credit Rating: ___		
BC / DR Plan	Dated: ___/___/___ Comprehensive? Y / N DR Site: None / Cold / Warm / Hot		
BCP / DRP Test Results	Date of Last Test: ___/___/___ Successful Recovery? Y / N Met RTOs? Y / N RPOs? Y / N		
Insurance Coverage	Liability Limits: _____/_____ Carrier: _____ Cybercrime? Y / N Business Resumption? Y / N "ACME" is Named Insured? Y / N		
PCI Data Security Standard	Type: Merchant / Service Provider PCI Level: 1 / 2 / 3 / 4 QSA: _____ ROC / AOC? Y / N Date: ___/___ SAQ: A / B / C / D Provided? Y / N		
Security Certification	Type: ISO 27001 / SysTrust / WebTrust / Other: _____ Certifier: _____ Date of Issue: ___/___/___		
Results of Independent Testing	Tests: Pen Test / Social Engineering / Vulnerability Scans Tester: _____ Report Date: _____ Satisfactory Results? Y / N		
Security Review	Security Questionnaire? Y / N Onsite Assessment? Y / N Offsite Assessment? Y / N Documentation Review? Y / N		
Security Incidents	Security Incidents Reported? Y / N Timely Notification? Y / N Addressed Satisfactorily? Y / N		
Performance Indicators	SLA / SLO Reports Received? Y / N SLA / SLOs Met? Y / N Complaints Noted? Y / N		

Risk Remediation Matrix

Notes: For the following items please indicate if you agree to remediate or not (Y/N). If no, please explain why not and what controls you already have in place to mitigate this risk. Also, if you have an alternative remediation plan that is in the same spirit as the proposed countermeasure, that can be implemented instead. The Target Date is established using "ACME" default guidelines. You can always remediate prior to the target due date.

#	Risk Description	Risk Rating	Recommendation	Response Due Date	Owner	Plan to Implement? Y/N	Comments	Alternate Remediation
1								
2								
3								
4								
5								
6								
7								
8								
9								
10								
11								
12								
13								
14								
15								
16								
17								
18								
19								
20								
21								
22								

Risk Acceptance Form

Risk Acceptance Form			Track #
To be completed by the ISMG Representative			
1. Date:	2. ISMG Representative:	3. Director of IT Security: (if different than ISMG Rep)	
4. Business Unit:		5. Chief Technology Officer:	

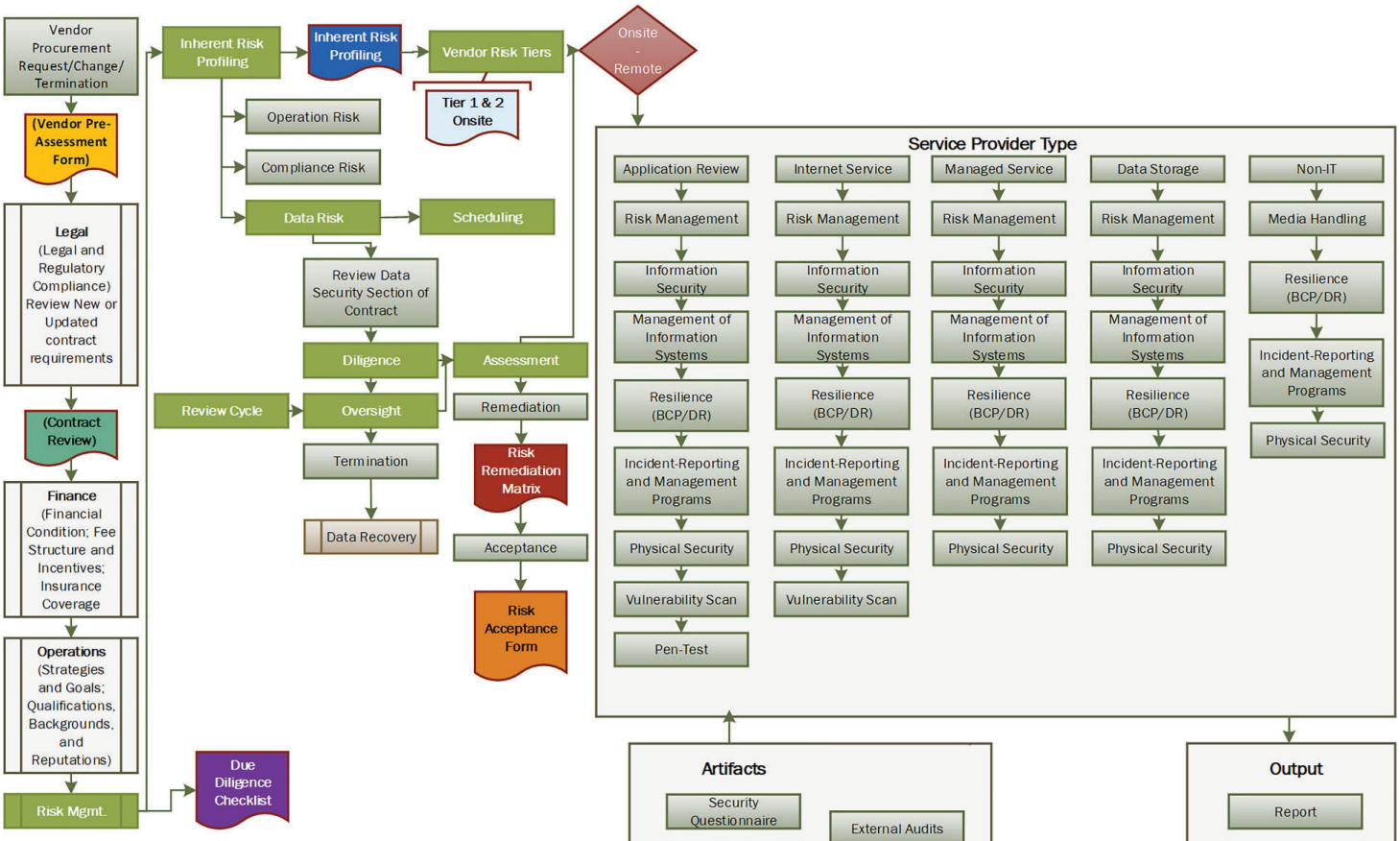
6. Technology Information (if applicable)				
Server Name	Operating System	Description	Location	Other Technology

To be completed by the ISMG Representative	
7. Description of Issue:	
8. Description of Risk:	
9. Compliance Violation, Policy, Standard, Technical Standard (List all that apply):	
10. Response to suggested mitigating controls or compliance plan (if applicable):	
To be completed by the Business/System Manager	
11. Description of Business Justification:	
12. Description of Mitigating Controls (if applicable):	
13. Plan to bring System, Application or Risk into Compliance (if applicable) (Include Timeframe):	

Business/System Owner:		Date:
ISMG Representative:		Date:
Legal Representative:		Date:
(C-Level Representative):		Date:

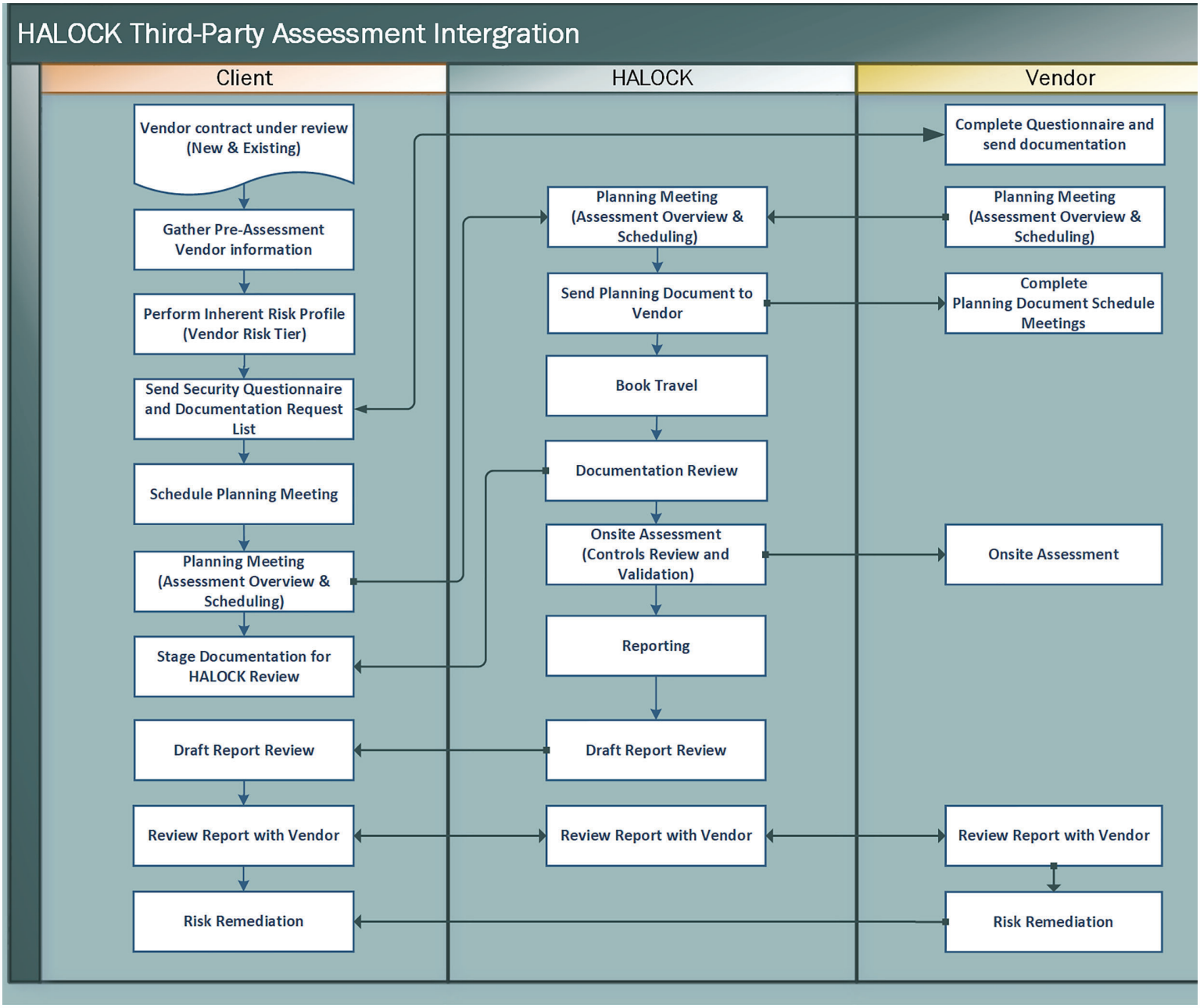
HALOCK maps the current vendor management processes to industry standards and proven risk management frameworks. Though HALOCK evaluates the program to the highest maturity model the goal of the assessment is to develop a portfolio of reasonable recommendations, and controls, to align heightened standards with the organization mission and compliances requirements. Working with risk management stakeholders the assessment focuses on:

- Roles and responsibilities within the risk management program
- Workflow reviews of vendor onboarding, oversight and termination.
- Organizations approach to assigning the inherent risk of third-party relations
- Vendor risk tiers definitions
- Vendor assessment process
- Personnel skillsets
- Current policies and framework



Third Party Risk Management Program Overview

Third Party Due Diligence Review Integration



HALOCK® FastStart Checklist

VENDOR RISK MANAGEMENT

HALOCK's FastStart Vendor Risk Management (VRM) Checklist allows organizations to initiate a formal VRM Program and get started immediately! The 6-step checklist defines the essentials to classify and manage vendors by risk and customize the on-boarding and audit process for each vendor classification tier. When the Board asks about risks posed by third parties, you can respond in business-friendly terms incorporating the organization's obligations, mission, and objectives… and confidently proclaim you are performing your due care!

ITEM 1 Engage Management

- ☐ **Identify Vendor Sponsors/Owners –** Identify who in your organization are the vendor sponsors and/or owners
- ☐ **Research/Build a Case –** Do some investigative research and build your case for management by gaining an understanding of how many vendors your company deals with, the types of vendors, the levels of complexity and quantities
- ☐ **Present Your Findings –** Describe your case for developing and operating a Vendor Risk Management Program to Executive Management

ITEM 2 Inventory & Classify Vendors

- ☐ Identify the various legal, regulatory and contractual obligations your organization has that applies to vendors
- ☐ Design and implement a series of vendor tiers; 3-5 is a good average
- ☐ Assign each vendor to a tier

ITEM 3 Define Assessment Process

- ☐ Determine what your organization's Calculated Acceptable Risk Definition is – and state it in plain English
- ☐ Create an assessment plan
  - ☐ Develop tier-specific questionnaires including questions for each process and the controls in use in order to fully understand how a control is being used, operated and monitored
  - ☐ Construct criteria for onsite and offsite evaluations
  - ☐ Create a prioritized assessment calendar
- ☐ Develop Vendor Risk Reporting format for Executive Management

ITEM 4 Develop Process for Risky Vendors

- ☐ Develop a set of options and procedures to address risk (e.g. change vendors, enforce contractual fines, pay or assist in remediation efforts, et al.)
- ☐ Develop process for following up on risk resolution and escalation (be sure you're closing the loop when a risk has been identified by ensuring the risk has been remediated)

ITEM 5 On-boarding & Contract Management

- ☐ Construct tier-specific contractual language, including penalties, enforcement, actions, et al.
- ☐ Develop on-boarding process for vendors
  - ☐ Understand expected level of sensitive data involved and nature of business
  - ☐ Assign vendor to tier, conduct baseline assessment, define remediation items required prior to operation, determine risk of not authorizing vendor
  - ☐ Distribute VRM Guide to potential vendor owners and procurement
  - ☐ Develop process for updating existing contracts with new requirements, penalties, etc.

ITEM 6 Monitor & Improve

- ☐ Integrate into overall risk management process (if one exists)
- ☐ Schedule recurring vendor management meetings with vendor owners to review vendor risk status
  - ☐ Report vendors outside of Calculated Acceptable Risk Definition
  - ☐ Obtain status on issue resolution
  - ☐ Report on assessment vendor coverage (on schedule, % complete, % fail, total outstanding risk items per vendor, et al.)

HALOCK®

HALOCK Security Labs
1834 Walden Office Square, Suite 200
Schaumburg, IL 60173
847-221-0200

Incident Response Hotline: 800-925-0559

www.halock.com

About HALOCK

Founded in 1996, HALOCK Security Labs is a thought-leading information security firm, that combines strengths in strategic management consulting with deep technical expertise. HALOCK's service philosophy is to apply just the right amount of security to protect critical assets, satisfy compliance requirements and achieve corporate goals. HALOCK's services include: Security and Risk Management (duty of care risk assessments), Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.