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 onboarding 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® Purpose Driven Security
847.221.0200 | info@halock.com | www.halock.com

NON EMERGENCY
847.221.0200
OFFICE

FOR EMERGENCIES
800.925.0559
INCIDENT RESPONSE HOTLINE