Third-Party Risk Management & Vendor Assessment Services

PROGRAMS | DELIVERABLES | INTEGRATION | FAST START CHECKLIST

Simplify Your Business. Secure Your Partners.

Ensure third-party partners are aligned with your organization's risk controls. Vendors and contractors serve as an extension of your business. They represent you and should operate under your business requirements.

Regulatory requirements and industry standards such as HIPAA, GDPR, ISO 27001, NIST 800-53, and numerous others require a risk-based third-party management program to protect the data shared with service providers and vendors.

Protect your customers, incorporate appropriate security standards as part of your contracts, and assess your future partners' ability to keep information secure. HALOCK can help build and manage a specific program for your environment.

VENDOR SELECTION DUE DILIGENCE

CONTRACTUAL SECURITY REQUIREMENTS

INHERENT RISK CRITERIA

VENDOR RISK TIERING

DILIGENCE AND OVERSIGHT

PRE-ASSESSMENT PLANNING

VENDOR ASSESSMENTS

RISK ACCEPTANCE AND TOLERANCE

HALOCK®

THIRD PARTY PROGRAM ASSESSMENTS

NEW PROGRAM DEVELOPMENT, CURRENT PROGRAM IMPROVEMENTS

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's mission and compliance 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

Organization's approach to assigning the inherent risk of third-party relations

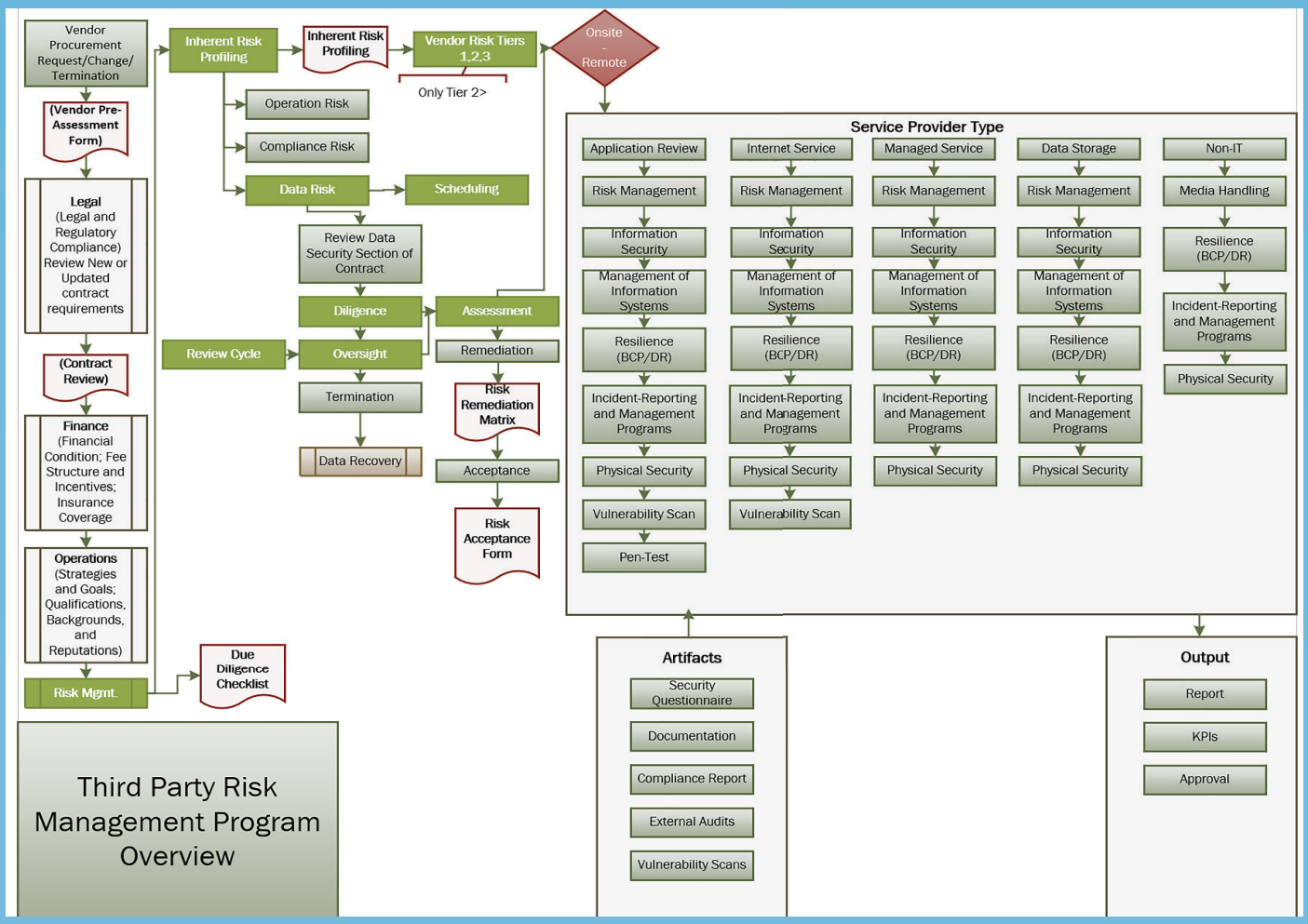
Vendor risk tier definitions

Vendor assessment process

Personnel skillsets

Current policies and framework

THIRD-PARTY RISK MANAGEMENT WORKFLOW



HOW DO YOU ALIGN TO A MATURE INDUSTRY STANDARD THIRD-PARTY RISK MANAGEMENT PROGRAM?

VENDOR SECURITY ASSESSMENTS

VENDOR SELECTION, REDUCE BACKLOG, INTEGRATED PROGRAM

HALOCK can integrate with your team to help assess your vendor's control environment for compliance with privacy and security requirements, reporting assessment results and presenting recommendations for high-risk services to remediate potential exposure of data and security breaches.

Strong knowledge of

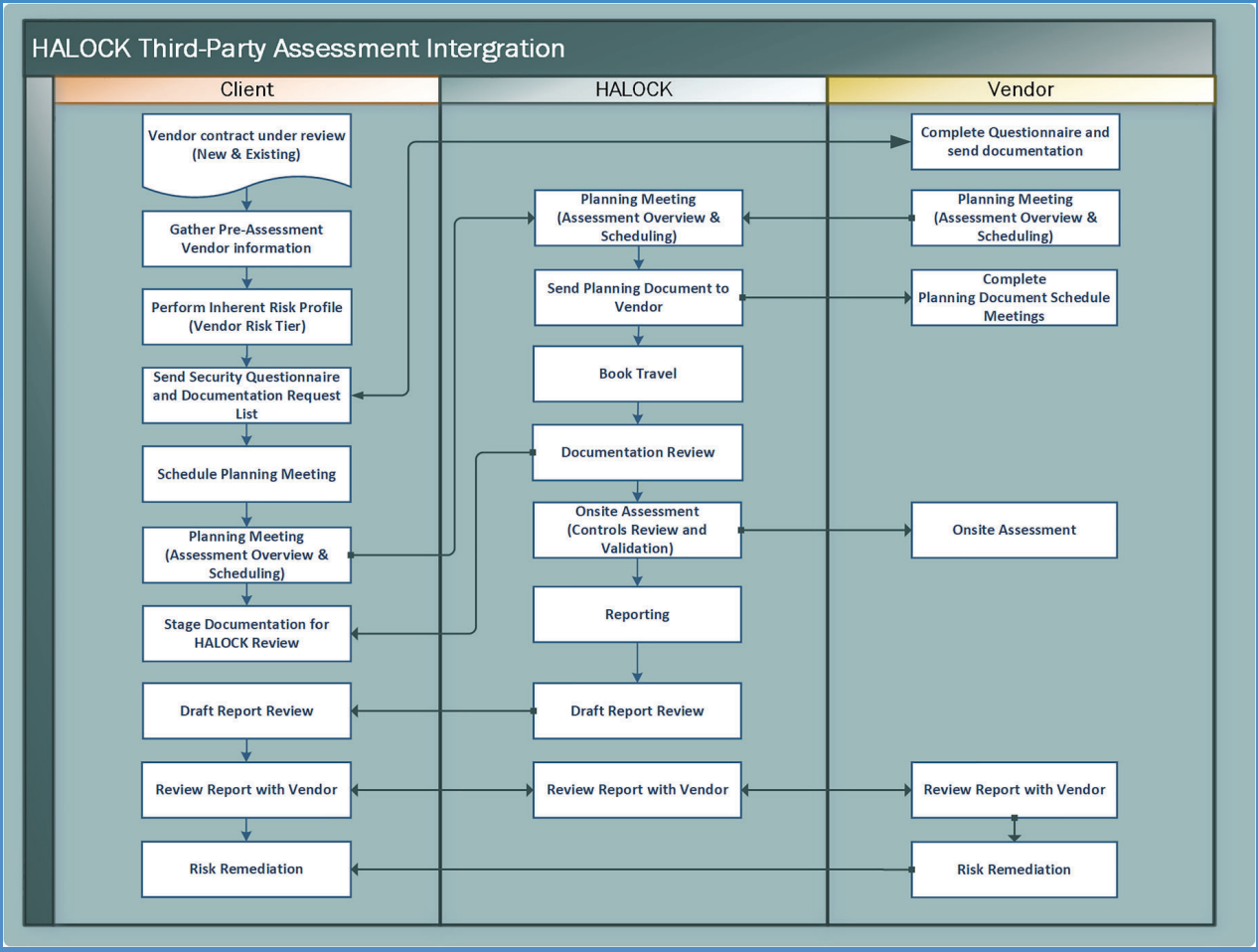
- Regulatory standards that govern Information Security practices such as HIPAA, PCI, GDPR, and state and federal privacy laws
- Information Security Risk assessment and analysis methodologies (FFIEC, NIST, etc.)
- Information security standards (ISO 27000 series, NIST, etc.)

Familiarity with Supplier Management GRC systems

Pool of Qualified Security Assessors

Ability to develop executive reports and deliver presentation to executives

VENDOR ASSESSMENT DUE DILIGENCE



ARE YOU ASSESSING YOUR THIRD-PARTY RELATIONSHIPS TO A LEVEL OF TRUST AND CONFIDENCE?

PROJECT HIGHLIGHTS

Vendor Request Form

<Vendor Name>

(This sheet should be completed internally by ACME before sending to the vendor)

ACME Project Management Information				
Requestors Name:	<NAME>			
Phone #:	<xxx-xxx-xxxx>			
Email:	<Project Manager Email Address>			
Date Requested	<xx-xx-xxxx>			
Vendor Information				
Vendor Name:	<Name>			
Contract #:	<ID #>			
Vendor Corporate Address:	<Street Address>	<City>	<State>	<Zip Code>
Location(s) to be Reviewed:	<Location Function/Description>			
	<Street Address>	<City>	<State>	<Zip Code>
	<Location Function/Description>			
	<Street Address>	<City>	<State>	<Zip Code>
	<Location Function/Description>			
	<Street Address>	<City>	<State>	<Zip Code>
	<Location Function/Description>			

Contract Review Checklist

Provision	Inquiries	Commentary / Observations	OK?
Scope of Service	Spells out obligations of both parties? Y / N		
Term	Term: __ years / Perpetual Reasonable length? Y / N		
Renewal	Auto-renewal? Y / N Notification required: ___ days		
Performance Standards	Includes warranties? Y / N SLAs / SLOs defined? Y / N Penalties defined? Y / N		
Confidentiality	Responsibilities defined? Y / N Exceptions defined? Y / N Survives relationship? Y / N		

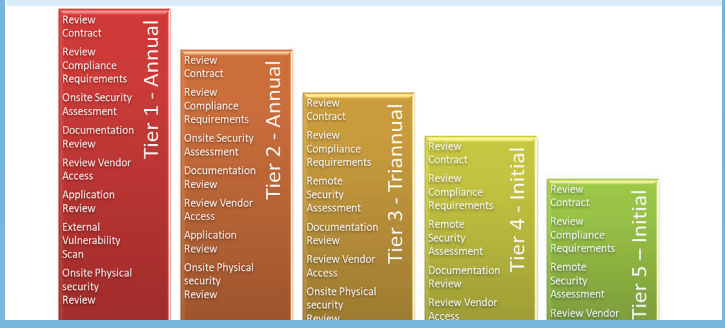
Due Diligence Checklist (Initial and Subsequent)

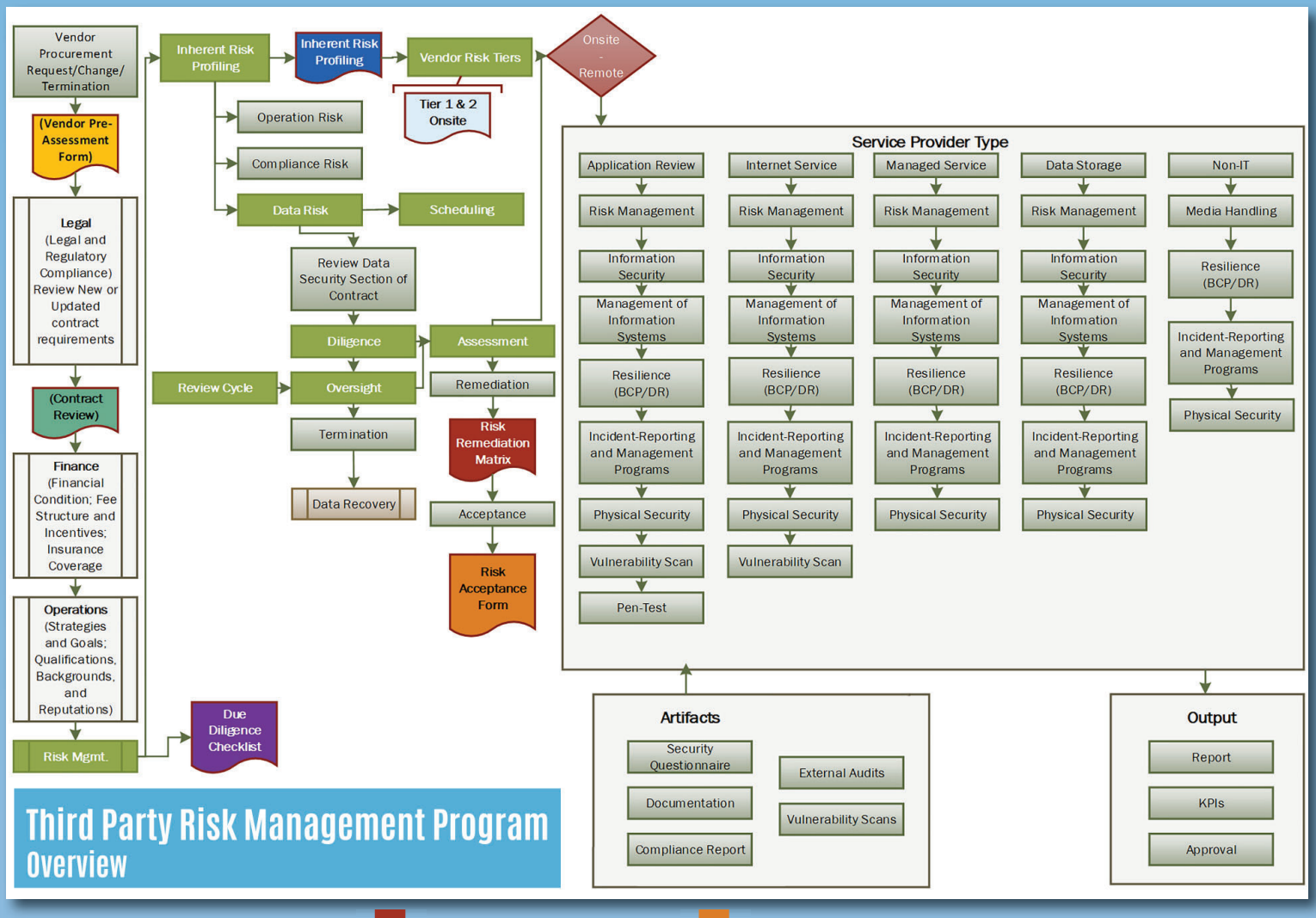
Item	Characteristics	Commentary / Observations	OK?
Legal Review	Contract Review: Y / N Compliance Review: Y / N		
Audit Report	SOC: 1 / 2 Type: I / II Auditor: _____ Test Period: ___/___ to ___/___ Opinion: Qualified / Unqualified Control Exceptions? Y / N		
Financial Statements and Credit Information	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		

Inherent Risk Profiling

Vendor:	Hyber Analytics		Inherent Risk:	High	
Date:	1/1/2019		Vendor Tier:	Tier 1	
Factor	Low	Minimal	Moderate	Significant	High
Type of information	No Data	Public infor-mation, non-regulated	Internal use only information (e.g., policies, proce-dures, routine memorandums)	Confidential infor-mation, intellectual property (trade se-crets).	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 con-tract	Statement of Work	Subject to contrac-tual requirements mandating the ex-ercise of due care	Subject to GLBA, SOX, FACTA, etc.	Subject to PCI DSS, FFIEC, HIPAA
Criticality of Service to Business	No SLA (Service Level Agreement) requirements	Services can be un-available for more than a month without materially disrupting "ACME"'s business	Services unavailability for one week to one month will materi-ally disrupt "ACME"'s business	Services unavailability for less than a week will ma-terially disrupt "ACME"'s business	Service unavailability for less than a day will ma-terially 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	Insecure file transfer to or	Vendor has direct access to

Vendor Risk Tiers - 1 & 2





Third Party Risk Management Program Overview

Risk Remediation Matrix

es: 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 prog

Risk Description	Risk Rating	Recommendation	Response Due Date	Owner	Plan to Implement? Y/N	Comments	Alternate Remediation

Risk Acceptance Form

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:	

HELPING YOUR GROWING BUSINESS STAY SECURE

WHY HALOCK?

RAPID PROGRAM REVIEW

HALOCK can review management requirements for third party information security assessments (inducing applicable regulations and standards), and design a proper assessment process that states the levels of scrutiny, including the associated processes and the requirements for the degree of due diligence the third parties must undergo based on their impact tier.

THIRD-PARTY RISK CONSULTANTS

HALOCK offers access to industry leaders in Risk Management and Vendor Security. Working in partnership with internal business drivers, HALOCK consultants use extensive career knowledge to help implement or reform the organization's management of risk created through third-party relationships. In addition to the program development practice, equipped with a wide range of security expertise, and knowledge of multiple compliance/standards requirements, HALOCK's consultants can perform independent vendor assessments to a degree not normally achievable by internal auditors.

DELIVERABLES & ARTIFACTS

CONTRACTUAL SECURITY LANGUAGE

PROGRAM FLOW CHARTS

INHERENT RISK CRITERIA

VENDOR RISK ANALYST CRITERIA

PRE-ASSESSMENT SCOPING WORKSHEETS

VENDOR ASSESSMENT PLANNING

SECURITY QUESTIONNAIRES

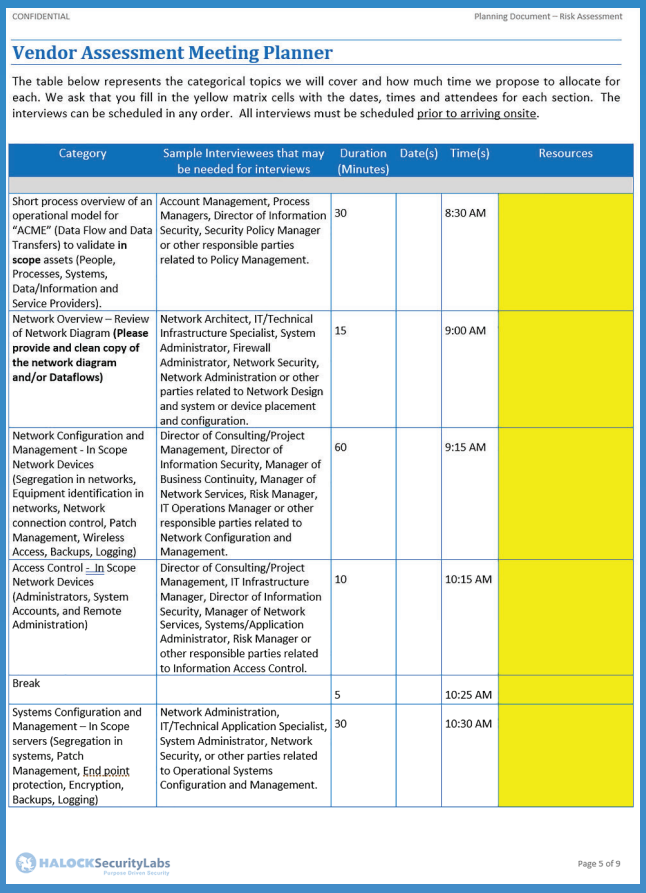
DOCUMENT REQUEST LIST

ASSESSMENT PLANNER

ASSESSMENT DETAILS

DOCUMENT REQUEST

EXECUTIVE SUMMARY



CONFIDENTIAL — Planning Document – Risk Assessment

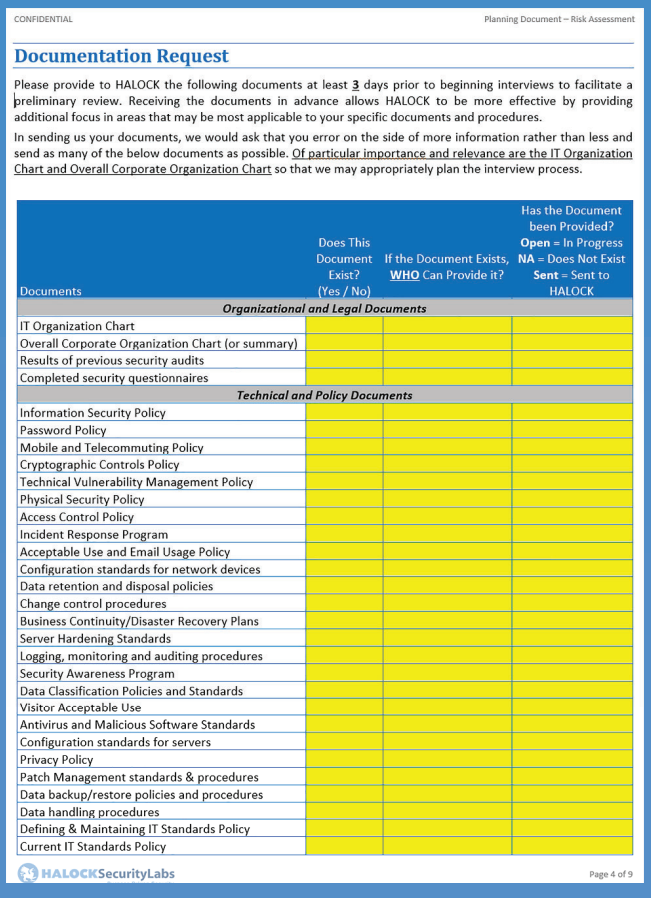
Vendor Assessment Meeting Planner

The table below represents the categorical topics we will cover and how much time we propose to allocate for each. We ask that you fill in the yellow matrix cells with the dates, times and attendees for each section. The interviews can be scheduled in any order. All interviews must be scheduled prior to arriving onsite.

Category	Sample Interviewees that may be needed for interviews	Duration (Minutes)	Date(s)	Time(s)	Resources
Short process overview of an operational model for "ACME" (Data Flow and Data Transfers) to validate **in scope** assets (People, Processes, Systems, Data/Information and Service Providers).	Account Management, Process Managers, Director of Information Security, Security Policy Manager or other responsible parties related to Policy Management.	30		8:30 AM	
Network Overview – Review of Network Diagram **(Please provide and clean copy of the network diagram and/or Dataflows)**	Network Architect, IT/Technical Infrastructure Specialist, System Administrator, Firewall Administrator, Network Security, Network Administration or other parties related to Network Design and system or device placement and configuration.	15		9:00 AM	
Network Configuration and Management - In Scope Network Devices (Segregation in networks, Equipment identification in networks, Network connection control, Patch Management, Wireless Access, Backups, Logging)	Director of Consulting/Project Management, Director of Information Security, Manager of Business Continuity, Manager of Network Services, Risk Manager, IT Operations Manager or other responsible parties related to Network Configuration and Management.	60		9:15 AM	
Access Control - In Scope Network Devices (Administrators, System Accounts, and Remote Administration)	Director of Consulting/Project Management, IT Infrastructure Manager, Director of Information Security, Manager of Network Services, Systems/Application Administrator, Risk Manager or other responsible parties related to Information Access Control.	10		10:15 AM	
Break		5		10:25 AM	
Systems Configuration and Management – In Scope servers (Segregation in systems, Patch Management, End point protection, Encryption, Backups, Logging)	Network Administration, IT/Technical Application Specialist, System Administrator, Network Security, or other parties related to Operational Systems Configuration and Management.	30		10:30 AM	

HALOCKSecurityLabs — Page 5 of 9

Assessment Planner



CONFIDENTIAL — Planning Document – Risk Assessment

Documentation Request

Please provide to HALOCK the following documents at least **3** days prior to beginning interviews to facilitate a preliminary review. Receiving the documents in advance allows HALOCK to be more effective by providing additional focus in areas that may be most applicable to your specific documents and procedures.

In sending us your documents, we would ask that you error on the side of more information rather than less and send as many of the below documents as possible. Of particular importance and relevance are the IT Organization Chart and Overall Corporate Organization Chart so that we may appropriately plan the interview process.

Documents	Does This Document Exist? (Yes / No)	If the Document Exists, **WHO** Can Provide it?	Has the Document been Provided? **Open** = In Progress **NA** = Does Not Exist **Sent** = Sent to HALOCK
Organizational and Legal Documents			
IT Organization Chart			
Overall Corporate Organization Chart (or summary)			
Results of previous security audits			
Completed security questionnaires			
Technical and Policy Documents			
Information Security Policy			
Password Policy			
Mobile and Telecommuting Policy			
Cryptographic Controls Policy			
Technical Vulnerability Management Policy			
Physical Security Policy			
Access Control Policy			
Incident Response Program			
Acceptable Use and Email Usage Policy			
Configuration standards for network devices			
Data retention and disposal policies			
Change control procedures			
Business Continuity/Disaster Recovery Plans			
Server Hardening Standards			
Logging, monitoring and auditing procedures			
Security Awareness Program			
Data Classification Policies and Standards			
Visitor Acceptable Use			
Antivirus and Malicious Software Standards			
Configuration standards for servers			
Privacy Policy			
Patch Management standards & procedures			
Data backup/restore policies and procedures			
Data handling procedures			
Defining & Maintaining IT Standards Policy			
Current IT Standards Policy			

HALOCKSecurityLabs — Page 4 of 9

Documentation Request

Executive Summary

ISO/IEC 27002:2013, Controls Review and Validation Summary

An initial set of onsite interviews and document reviews called the "Controls Review," helped HALOCK understand vendor's security controls environment. Topics such as access controls, auditing, technical safeguards, business continuity, and security standards were discussed as they relate to the services provided.

Additionally, HALOCK reviewed and observed vendor's existing security controls during "Controls Validation." HALOCK selected a set of security controls and assets to assess. Controls validation activities included technical snapshots of system configurations, eyes-on review of system configurations, evaluation of evidence of management review of controls and processes, and process walk-throughs with personnel.

HALOCK used ISO/IEC 27002:2013 controls as a baseline to measure the maturity of the vendor's information security program against an accepted industry standard. HALOCK interviewed key personnel to determine how well the design and intent of information security controls conform to the controls that are in the ISO 27002 Security Controls Definition. Using 5 levels of maturity (1-Initital, 2-Repeatable, 3-Defined, 4-Managed, 5-Optimizing), HALOCK rated each ISO 27002 Security Control according to its maturity level, where a maturity level of 3 or higher is acceptable.

Vendor's Overall Information Security Program Maturity

3-Defined (institutionalized)	*(Define Statement Vendor's)*

Clauses		Clauses	
A.5.1 information security Management	3	A.12.3 Backup	4
A.6.1 Internal organization	3	A.12.4 Logging and monitoring	3
A.6.2 Mobile devices and teleworking	2	A.12.5 Control of operational software	3
A.7.1 Prior to employment (Screening)	4	A.12.6 Technical vulnerability management	3
A.7.2 During employment (Security Awareness)	4	A.12.7 Information systems audit considerations	3
A.7.3 Termination and change of employment	3	A.13.1 Network security management	3
A.8.1 Responsibility for assets (Asset Management)	3	A.13.2 Information transfer	3
A.8.2 Information classification	3	A.14.1 Security requirements of information systems	3
A.8.3 Media handling	3	A.14.2 Security in development	3
A.9.1 access control	3	A.14.3 Test data	3
A.9.2 User access management	3	A.15.1 Information security in supplier relationships	3
A.9.3 User responsibilities	3	A.15.2 Supplier service delivery management	3
A.9.4 System and application access control	3	A.16.1 Management of information security incidents	2
A.10.1 Cryptographic controls	3	A.17.1 Information security continuity	3
A.11.1 Secure areas (Physical Security)	3	A.17.2 Redundancies	3
A.11.2 Equipment	3	A.18.1 legal and contractual requirements	3
A.12.1 Operational procedures and responsibilities	3	A.18.2 Information security reviews	2
A.12.2 Protection from malware	3		

1. Initial (chaotic, ad hoc, heroic): The starting point for the use of a new process.
2. Repeatable (project management, process discipline): The process is repeatedly used.
3. Defined (institutionalized): The process is defined/confirmed as a standard business process.
4. Managed (quantified): Process management and measurement take place.
5. Optimizing (process improvement): Process management includes deliberate process optimization/improvement.

*Note: The maturity model does not represent the risk associated with the services provided by Client.

Executive Summary

Vendor Assessment Risk Details

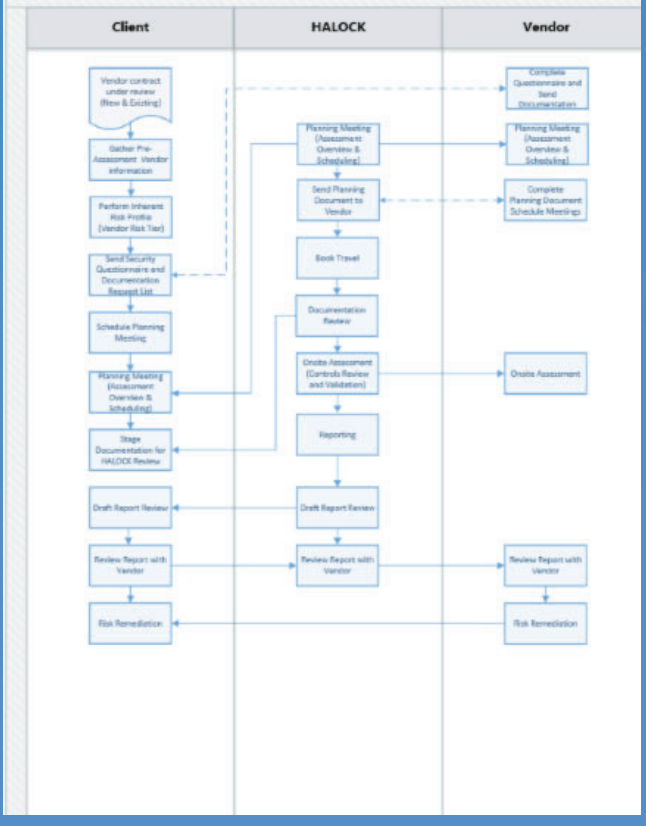
Risk #	Vulnerability Identified	Existing Countermeasures	Likelihood	Impact	Risk
1	Technical controls to restrict transfer of software from development to production status are not defined, implemented, or documented i.e. no formal program release manager.	Five developers can push their own changes to AWS production network.	4 - Very Likely	4 - High	16
	Proposed Remediation	**Alternate Remediation Proposed by Vendor**	**Implement Yes/No**	**Status**	**Due Date**
	Program source code and the program source libraries should be managed and accessed only according to the organization's established procedures (i.e., change management).				

Risk #	Vulnerability Identified	Existing Countermeasures	Likelihood	Impact	Risk
2	The organization has not implemented any controls to restrict the use of unauthorized software. Controls may include, but are not limited to: - Restricting local administrator rights on end-user workstations - Deploying automated software inventory and software management systems - Monitoring employee internet activity - Disabling/disallowing removable media devices	ACME user utilizes BYOD workstation with Ubuntu OS.	5 - Imminent	3 - Medium	15
	Proposed Remediation	**Alternate Remediation Proposed by Vendor**	**Implement Yes/No**	**Status**	**Due Date**
	All systems should be centrally management and anti-virus should be installed to prevent against know malicious software.				

Risk #	Vulnerability Identified	Existing Countermeasures	Likelihood	Impact	Risk
3	Anti-virus software used on internal BYOD systems is not formally implemented, centrally managed, and/or required on all systems.	Trend Micro is the company standard anti-virus software utilized internally.	4 - Very Likely	3 - Medium	12
	Proposed Remediation	**Alternate Remediation Proposed by Vendor**	**Implement Yes/No**	**Status**	**Due Date**
	All systems should be centrally management and anti-virus should be installed to prevent against know malicious software.				

Assessment Details

HALOCK Third-Party Vendor Management Engagement



Integration

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	Speedlezz	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

Service Provider Inventory

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, Compliance Validation, Penetration Testing, Incident Response Readiness, Security Organization Development, and Security Engineering.