Third - Party Governance Done Right

Brenda Ward
Director - Global Information Security

May 13, 2015
Several controls added to the Third Party Governance Process specifically address cyber security risks:

<table>
<thead>
<tr>
<th>CONTROL</th>
<th>TYPE</th>
<th>DETAIL</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard Information Gathering Tool (SIG)</td>
<td>Questionnaire</td>
<td>Full SIG for Hosting Vendors</td>
</tr>
<tr>
<td>Agreed Upon Procedures (AUP)</td>
<td>Controls Assessment</td>
<td>93 Controls Reviewed by 3rd Party</td>
</tr>
<tr>
<td>vBSIMM</td>
<td>Software Security Maturity Assessment</td>
<td>Performed by Assessor</td>
</tr>
<tr>
<td>Binary Static Scan</td>
<td>Vulnerability Scan</td>
<td>Conducted by 3rd Party and Shared with Assessor</td>
</tr>
<tr>
<td>Security Performance</td>
<td>Controls Assessment</td>
<td>Controls Obtained Through Network Scanning of Internet Facing Endpoint</td>
</tr>
</tbody>
</table>
# Third Party Risk Category Grid

<table>
<thead>
<tr>
<th>DESCRIPTION</th>
<th>A</th>
<th>B</th>
<th>C</th>
<th>D</th>
<th>E</th>
<th>F</th>
</tr>
</thead>
<tbody>
<tr>
<td>HOSTS RESTRICTED OR CONFIDENTIAL DATA</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HOSTS PROPRIETARY DATA</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>SOFTWARE DEVELOPMENT</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>HAS ACCESS TO DATA</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>-</td>
<td>-</td>
</tr>
<tr>
<td>MOBILE APPLICATION DEVELOPMENT</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>COMMERICAL OFF THE SHELF (COTS) SOFTWARE</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>NETWORK DIAGRAM/MAP</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>vBSIMM</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>CODE SCAN (VAST)</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>ENCRYPTION REVIEW</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>AUTHENTICATION REVIEW</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>3 POINT BACKGROUND CHECK</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
<tr>
<td>SECURITY SCORECARD</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
It is critical to start Third Party Risk Governance early to provide vendors time to complete the requirements involved in the Information Security Risk Assessment.

**CRITICAL WORKFLOW OF ANY THIRD PARTY IT RISK GOVERNANCE PROGRAM**

- **Request Mgmt Process**
- **Risk Category Process**
- **Assessor Assignment Process**
- **Vendor Artifact Submittal Process**
- **Artifact Assessment Process**
- **Approval & Exception Process**
- **Remediation Action Item Tracking Process**

<table>
<thead>
<tr>
<th>Process</th>
<th>Timeframe</th>
</tr>
</thead>
<tbody>
<tr>
<td>Request Mgmt Process</td>
<td>1 Day</td>
</tr>
<tr>
<td>Risk Category Process</td>
<td>1 Day</td>
</tr>
<tr>
<td>Assessor Assignment Process</td>
<td>Up to 6 Weeks</td>
</tr>
<tr>
<td>Vendor Artifact Submittal Process</td>
<td>20 Days</td>
</tr>
<tr>
<td>Artifact Assessment Process</td>
<td>3 Days</td>
</tr>
<tr>
<td>Approval &amp; Exception Process</td>
<td>Ongoing</td>
</tr>
</tbody>
</table>
Where to start...

Program Key Performance Indicators (KPIs)

- Vendor Submittals (Process A / B / C / Other)
- Vendor Request Intake (Submitted)
- Vendors in Progress
- Vendor Completion
- Vendors Not Approved
- Vendors Completed with Action Items (Remediation)
- Vendor Kickoff Meetings

Relationship Manager & Compliance Ownership


- < ?? Hours
- < ?? Days
- < ?? Days
- < 90 Days from Contract Sign Date

Process A
Process B
Process C
Process (2016)
Process (2016)
Other Processes (2016)
Implement: Information Classification Model

CONFIDENTIAL INFORMATION

- Protected Health Information (PHI)
  - Medical Records
    - Diagnosis & Procedure Codes
    - Lab Results
    - Claim Data
    - Etc.
- Personally Identifiable Information (PII)
  - Name, Address
  - Street, City, State, Zip Code
  - Member ID
  - DOB
  - Telephone & Fax Numbers
  - Email Addresses
  - Etc.
- Company Financial Data
- Merger & Acquisition Data

• Controls Meet All HIPAA & Other Regulatory Requirements
  - Nothing changes

RESTRICTED DATA:

- Credit Card Data
- SSN
- Credentials
  - User IDs & Passwords

New Controls:

- Encryption or Tokenization
- 2 Factor Authentication
- Increased Auditing & Monitoring
I like the fact that Company X is working to help the industry remove the need to complete assessments by providing the opportunity to complete one SIG and use it for additional engagements”, stated by multiple Vendors

- Awareness of vendor IT and Data Security vulnerabilities
- SIG Master is compared to the Vendor SIG for vulnerabilities to be remediated
- Remediation action items for vulnerabilities tracked to completion and re-assessed for sign off / accountability
Agreed Upon Procedures (AUP)

- Used to evaluate controls that vendors have in place
- Developed under the American Institute of Certified Public Accountants (AICPA) professional standards
- The Assessment includes:
  - Objective tests of controls
  - Validation of vendor self-assessment (SIG or SIG Lite)
  - Standardized Reporting
  - Results are captured in a Final Assessment Report and provided directly to the vendor
  - The Vendor can then share the report with any number of clients

Typical AUP Engagement = 6 to 8 Weeks

REMEDIATION ACTION ITEMS STORED IN TRACKING TOOL & DOCUMENTED IN CONTRACTS
Typical Assessment Timeline

Week 1:
- Set Expectations - Educate about AUP conduct
- Discuss/Confirm In-Scope Assets, Locations
- Discuss On-site dates

Week 2:
- Review D.x Inventory and destruction
- Review E.x HR (and H.2)
- Confirm On-site dates
- Review F.x DC perimeters

Week 3:
- Discuss lead-time items: account creation, password change
- Review System Controls G.x
- Review Access Controls H.x
- Review Doc needs for A, B, C, K,

Week 4:
- Review System Dev and Maint I.x
- Inc Mgt J.x
- Sub Vndr Mgt M.x
- Privacy P.x
- Confirm readiness
- Begin advanced review of documents

Week 5:
- CONDUCT ON-SITE ACTIVITIES
  - Ensure any/all OPEN items are identified for resolution
  - Any items not resolved in 1 week will be immortalized in final letter

Week 6:
- Resolve all open items
- DRAFT Final Report
- Complete Final Report

AUP Review and Education
Advanced Doc Rvw
Confirm Readiness
On-Site Activities
Resolve Open Items
Final Report
AUP vs SOC2

- Determine a single control standard
- Determine if supplemental documentation will be accepted
- Engage a third party vendor as a preferred vendor
- Understand the difference between the AUP and the multiple types of SOC(s)

3rd Party Risk Governance Program – Agreed Upon Procedures (AUP) FAQ

Why a Shared Assessment AUP rather than a SOC 2?

- Consistency in scope – Under the 2014 version, every AUP Assessment will include the same set of 80 control tests when assessing the Target Systems. Some control tests may be determined to be ‘Not Applicable’. However, the assessed vendor does not unilaterally influence control tests that are in scope. In some assessment scenarios outside of the AUP, the assessed vendor themselves can choose [only] a subset of principles to be assessed.
- Consistency in test procedures – The AUP prescribes the procedure[s] to be used for each control test. This ensures consistency across assessments of different vendors, performed by different assessors.
- Elimination of Assessor Opinion – The AUP uses consistent, prescribed test procedures for each control. Additionally, the reporting of results is limited to stating that specific attributes are either ‘Present’ or ‘Not Present’. Assessor opinions of the effectiveness of controls are not included in an AUP report.
- Portability of the Final Report – The Shared Assessments Program does not place any limitations on the sharing of an AUP Report. Some other report formats come with limitations on who can access or share a report. The AUP Report and process allows for complete and open sharing of reports.
- Availability of Assessment Firms – Only a Certified Public Accounting firm can perform a SOC 2 engagement. No such restrictions exist on who can perform a Shared Assessments AUP.

Can I submit an AUP Report from my AICPA firm?

Yes, you can. However, the Shared Assessments AUP Report format may not be acceptable for use by your AICPA firm. If your firm uses an alternate format, all tests must be conducted as stated in the Shared Assessments AUP and the report must clearly show the objective results of EACH control test as listed in the Shared Assessments AUP Table of Contents.

Can I submit an AUP Report as part of a SOC 2-plus Report?

The SOC 2-plus is a recent and evolving topic. Its effectiveness and acceptance in the industry is not yet known, especially to address the specific needs of a Shared Assessments AUP Report. If this artifact (SOC 2-plus) is used to cover the AUP needs, the test procedures that contribute to the AUP MUST be conducted as stated in the Shared Assessments AUP, and the final report to address the AUP requirement MUST clearly show the objective results of EACH control test as listed in the Shared Assessments AUP Table of Contents.

Areas of focus for these assessments include internal and external account management, password policies, authorization models, and other supporting identity and access management controls.
Vendor BSIMM (vBSIMM)

vBSIMM PROCESS AREAS:
1. Architecture Analysis
2. Code Review
3. Security Testing
4. Penetration Testing
5. Configuration Management – Incident Response / Vulnerability Management

ASSESSMENT & INITIAL SCORING SYSTEM:
- Top Total Score = 15 points
- Top Total Score for each area = 3 points
  - 0 = Not Implemented
  - 1 = Low Maturity
  - 2 = Medium Maturity
  - 3 = High Mature

Control Accomplishments
- Awareness of vendor software development vulnerabilities
- Training provided to vendor to improve maturity
  “Thank you for taking the time to teach us the process and the areas where our software development can be improved”, Vendor
- Remediation action items for vulnerabilities tracked to completion and re-assessed for sign off / accountability

ASSESSOR & VENDOR REVIEW
MTG

FINAL ACTION ITEM & SCORING

eGRC TRACKING TOOL

REMEDIATION ACTION ITEMS STORED IN TRACKING TOOL & DOCUMENTED IN CONTRACTS
What is vBSIMM?
Simply put, vBSIMM is an assessment process that provides visibility into the maturity of a vendor’s ability to deliver secure software by evaluating.

vBSIMM Practices
(1) Architecture Analysis Activity
Vendor performs security design / architecture / feature review (threat models).
(2) Code Review Activity
Vendor uses automated tools and/or manual review.
(3) Security Testing Activity
Vendor ensures QA supports edge/boundary value condition testing.
(4) Penetration Testing Activity
Vendor uses penetration testers to identify security vulnerabilities.
(5) Configuration Management - Incident Response / Vulnerability Management
Vendor uses vulnerability/ incident data to modify security practices (prevention).
Two Options Provided To Vendors:
1. Successful completion of vBSIMM Assessment AND provides an application vulnerability report of sufficient detail generated by an approved assessment tool.
2. Completion of a code assessment process facilitated by a 3rd Party.
The intent is to provide awareness to vulnerabilities and help uplift vendors' security posture to the maturity of your company.
## Estimated Artifact Timelines

<table>
<thead>
<tr>
<th>ARTIFACT</th>
<th>APPROX. TIMELINE TO COMPLETE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>FULL SIG</td>
<td>4 weeks</td>
<td>Fill out questionnaire (Approx. 1,500 questions)</td>
</tr>
<tr>
<td>SIG LITE</td>
<td>1 week</td>
<td>Fill out questionnaire (Approx. 125 questions)</td>
</tr>
<tr>
<td>AUP</td>
<td>6 weeks</td>
<td>After or in concert with SIG or SIG Lite. Engagement with Third Party Assessor. Six week timeline requires very focused participation and approximately four days on site assessment. Final Assessment Report Required</td>
</tr>
<tr>
<td>NETWORK MAP</td>
<td>Vendor Driven</td>
<td>Vendor to provide documentation if requested</td>
</tr>
<tr>
<td>vBSIMM</td>
<td>4 weeks</td>
<td>Includes a 1 hour vBSIMM review meeting to discuss submitted artifacts</td>
</tr>
<tr>
<td>CODE SCAN</td>
<td>4 weeks</td>
<td>Appropriately scoped Penetration Test based on complexity of Application: - Static Binary Application Scan (SAST) - Development Cycle (Preferred) - Dynamic Application Scan (DAST) - Testing Cycle</td>
</tr>
<tr>
<td>ENCRYPTION RVW</td>
<td>30 minutes</td>
<td>Fill out questionnaire (Approx. 20 questions)</td>
</tr>
<tr>
<td>AUTHENTICATION RVW</td>
<td>30 minutes</td>
<td>Fill out questionnaire (Approx. 20 questions)</td>
</tr>
<tr>
<td>3 POINT BACKGROUND</td>
<td>1 hour</td>
<td>Assessor completes a 3 point background check and will contact the vendor if vulnerabilities are found</td>
</tr>
<tr>
<td>SECURITY PERFORMANCE</td>
<td>24 hours</td>
<td>Assessor reviews your Security Performance</td>
</tr>
</tbody>
</table>
Implement: Approval Process

Approved
Approved with Remediation Action Items
Not Approved (Rejected)
Withdrawn by Procurement
Withdrawn by the Business

By Category

Remediation
Action Item
Management
Process

Exception Process
THIRD PARTY GOVERNANCE

Vendor ISAC Portal

eGRC TRACKING TOOL

VENDOR ISAC PORTAL
- Blogs / Vlogs
- Email Campaign
- Content Management
- Mobile Web Versions
- Email Integration
- Bilingual Functionality

THIRD PARTY UNIVERSE

BUSINESS

EVALUATION

RFP

EVM

STRATEGIC PORTFOLIO

LAW FIRMS

vBSIMM & CTPRP Certification

CONSISTENT VENDOR COMMUNICATION

VENDOR COMMUNITY

4TH PARTY VENDORS

5TH PARTY VENDORS

6TH PARTY VENDORS

THIRD PARTY UNIVERSE

* 3rd Party Universe includes: vendors/suppliers, delegates, providers (which may or may not be delegates), joint venture partners (which may or may not be 4th Party), etc.
The Vendor Community

Organization A

Organization Attacked

NH-ISAC
Community Repository

FS-ISAC
Community Repository

Automated Defense

Organization B

Many Trusted Organizations Protected

Even More Trusted Organizations Protected
Threat Intelligence Platform (TIP)

Automated Threat Feed

Web Root  Virus Total  ISAC STIX / TAXII

STIX

SOLTRA

TAXII

TAXII

Trusted Circle

Anonymous Remote Query and Alerting Across NH-ISAC

“Neighborhood Watch”

Auto Query on STIX Data

Supported SIEM’s
- HADOOP
- ARC Sight
- Q-Radar
- RSA SA
- Splunk
- Log Stash/Elastic Search

Vorstack Local ACP

SIEM
Implement a rotational staff of Third Party Risk Governance Assessors.
Assessor Certification and Training

Vendor Building Security In Maturity Model (vBSIMM) Certification

- What vBSIMM is and is not
- 5 practices
- Interview objectives
- Common implementation approaches (positive signs and red flags)
- Scoring guidelines
- SDLC artifacts

Shared Assessments Certified Third Party Risk Professional (CTPRP)

- Managing the vendor lifecycle
- Vendor risk identification and rating
- Knowledge of the fundamentals of vendor risk assessment, monitoring, and management
- Standard Information Gathering Tool
- Agreed Upon Procedures

24 vBSIMM 23 CTPRP
Certified Assessors
Thank you

Contact Information: bkward1@aetna.com