Vendor Due-Diligence &
Vendor Management
Eclectic Guidance: Cybersecurity, Privacy & Validated Systems

Matt Stamper, Virtual CISO
CISO in Residence – CyberFlow Analytics
Proud Member of ISACA
MPIA, MS, CISA, CIPP-US, ITIL
Matt.stamper.eag@gmail.com / mstamper@cyberflowanalytics.com
Agenda

- Organizational domains
- The *inter-dependent* organization
- Vendor-Management Defined
- Our Current Vendor-Management Toolbox
- Why Vendor Management is So Important
  - Mandated by law
  - Good governance
- Multi-disciplinary approach:
  - Cybersecurity
  - Privacy Practices
  - CFR 21 Part II (Validated Systems)
- Due Diligence Basics...a Data Center Example
- Moving forward...
Organizational Domains

Most Organizations have functional, line-of-business, domains:

- Finance & Accounting
- Sales & Marketing
- Operations
- General & Administrative
- IT

For small-to-medium enterprises (SMEs), there are some important functions that are typically lacking and frequently outsourced:

- Privacy
- Security
- Vendor Management
No Organization is an island

Acme, Inc. Global HQ

Legal Services
Independent Contractors
Payroll Services
Business Process Outsourcing (BPO)

IT Services (Cloud & SaaS)
Strategic Vendors
HR Services
Application Development
Vendor Management Defined

“A vendor is a third party that supplies products or services to an enterprise. These products or services may be outsourcing, hardware, software, services, commodities, etc. Vendor management is a **strategic process** that is dedicated to the sourcing and management of vendor relationships so that **value creation is** maximized and **risk to the enterprise is minimized**” (Vendor Management Using COBIT® 5).
Vendor-Management Lifecycle

- Requirements Definition
- Selection Process & Criteria
- Contracting
- Implementation
- Management & Operations
- Transition or Service Termination
Triaging & Assessing Vendor Risk

Not all vendors are created equal. Good vendor-management practices recognize that not every vendor requires the same level of scrutiny and diligence. Vendors and prospective vendors should be assessed based on their inherent risk profile:

- Reputational Risk
- Financial Risk
- Operational Risk
- Regulatory Risk
- Privacy Risk
- Environmental Risk
- Legal Risk
- Other

There are a couple of key questions that should help put a given vendor’s risk profile in context:

- If our organization shares sensitive or regulated information (PII, ePHI, or cardholder data) with the vendor and there’s a breach, what are the consequences?
- If our organization’s operations rely on the availability of the vendor’s services and there is a service interruption, what are the consequences?
- If our vendor goes out of business, what are the consequences?
If we are charged to assess vendors in our organization’s ecosystem, here’s what’s likely in our current toolbox:

- **Formalized RFP**
  - Metric: Percentage of vendor-projects with defined requirements documentation
- **SSAE 16 Reports**
  - Metric: Percentage of Vendors who have been SSAE 16 audited with zero exceptions
- **Right-to-Audit Clauses**
  - Metric: Percentage of contracts with right-to-audit clauses and audits conducted
- **Reference Checks**
  - Metric: Percentage of selected vendors where references were checked in advance
- **Ad-hoc teams**
  - Metric: Percentage of vendors selected by formal vendor-management practice
- **Risk assessments**
  - Metric: Percentage of vendors who have been evaluated for various risk factors
Legally-Mandated Diligence

For many industries, an assessment of a vendor’s practices is not optional.

**Financial Services:**
- Federal Financial Institutions Examination Council (FFIEC)
- Gramm-Leach-Bliley: Section (501b)

**Healthcare:**
- HIPAA-HITECH: 164.308(b)(1)
HIPAA-HITECH in some detail:

- § 164.308 Administrative safeguards. (a) A covered entity or business associate must, in accordance with § 164.306:
  
  (1)
  (i) **Standard: Security management process.** Implement policies and procedures to prevent, detect, contain, and correct security violations.
  (ii) **Implementation specifications:**
    
    (A) **Risk analysis (Required).** Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.
    
    (B) **Risk management (Required).** Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).
    
    (C) **Sanction policy (Required).** Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.
    
    (D) **Information system activity review (Required).** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.
  
  (2) **Standard: Assigned security responsibility.** Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.
Good governance: IIA & ISACA

For other industries where vendor-management practices are not mandated, fiduciary responsibility and good governance practices are important. Our members offer great insights on vendor-management best practices:

https://global.theiia.org/knowledge/Public%20Documents/TaT_April_2014.pdf

Multi-disciplinary Approach

Leveraging insights and tools from other disciplines improves our overall vendor-management efforts. Here are some of the key contributions:

- Cybersecurity – Inspect what you expect, trust & identity
- Privacy - Data flow diagrams & data classification
- Validated Systems – Defined Requirements & Specifications

As we build our vendor-management practice, think about the proverbial blind spots in our analyses that can be illuminated by incorporating a slightly different perspective.
Leveraging alternative disciplines to think about Vendor management
Cybersecurity & Vendor Management

Confidentiality

Integrity

Availability

CIA
Good cybersecurity is a multi-disciplinary domain that extends beyond network security. Cybersecurity practices assume an inter-connected enterprise and these connections should always be questioned:

- Vulnerability scans
- Penetration testing
- Trust & Identity Management
- Authentication
- Anomalous Behavior
- Incident Response
- Forensics
What Privacy Offers...

<table>
<thead>
<tr>
<th>Respecting individual rights and choices around the <strong>data-privacy lifecycle</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Cross-border transfer rules</strong></td>
</tr>
<tr>
<td><strong>Notice &amp; Choice</strong> (opt-in &amp; out)</td>
</tr>
<tr>
<td><strong>Collection</strong></td>
</tr>
<tr>
<td><strong>Purpose &amp; Use</strong></td>
</tr>
<tr>
<td><strong>Access</strong></td>
</tr>
<tr>
<td><strong>Availability, Correction &amp; Quality</strong></td>
</tr>
<tr>
<td><strong>Disclosure, Sharing &amp; Forward Transfer</strong></td>
</tr>
<tr>
<td><strong>Storage, Retention &amp; Secure Disposal</strong></td>
</tr>
</tbody>
</table>

SoCal Privacy Consultants / www.SoCalPrivacy.com
What Privacy Teaches...

Information privacy practices, similar to cybersecurity, also leverages a multi-disciplinary approach. Some of valuable contributions of privacy include:

- Data flow diagrams
- Program and policy review
- Regulatory review
- Data lifecycle
Validated Systems
CFR 21 Part 11

Our colleagues in Pharma offer some great insights and contributions to vendor management. Specifically, the notion of “validated” systems is focused on the elimination of variance and quality throughout the GAMP lifecycle.

- User-Specification Requirements
- Functional Specification
- Design Specification
- System Build
- Install Qualification (IQ)
- Operational Qualification (OQ)
- Performance Qualification (PQ)
Multi-Disciplinary Approach

Vendor management requires the skills, insights, and expertise of multiple organizational disciplines:

- Line-of-Business
- Finance & Accounting
- Legal
- Internal Audit
- IT
- Security
Real-world Example:
Data Center & Managed Services
UPS
Due Diligence

UPS — specifically batteries — are responsible for many data center outages.

What should you assess:
✓ Age of batteries
✓ Monitoring of batteries
✓ Testing of batteries
✓ Capacity
✓ Configuration
  ▪ N
  ▪ N+1
  ▪ 2N
  ▪ 2n + 1
✓ Run time at peak load
✓ Support contracts
Generators
Due Diligence

Generators are an integral part of a data center’s electrical system.

What should you assess:
✓ Load testing
✓ Maintenance records
✓ Capacity
✓ Configuration
  ▪ N
  ▪ N+1
  ▪ 2N
  ▪ 2n + 1
✓ Support contracts
Network Operations
Due Diligence

NOCs function as the eyes and ears for IT service delivery.

What should you assess:

- Staffing levels & competencies
- Systems of record
- Training records
- HR Policies & Background Checking
- Mean-Time-to-Respond
- Monitoring Tools
- Escalation Procedures
- IR Procedures
- BIAs & BC/DR Plans
Storage & Services

SANs and backup infrastructure hold our organization’s critical information.

- Is the SAN and other infrastructure adequately maintained?
- How is performance of the SAN measured?
- What is the current available capacity?
- How many controllers and what are their performance metrics?
- How quickly can new capacity be added?
- Is the data encrypted?
- Who manages the keys?
- Where are backups maintained?
- Will our backup windows be met?
- Are backups encrypted?
- Are backups off-site?
Network & Security Services

Network and security services are critical components to most service delivery.

- What hardware is used by the provider?
- Are there maintenance contracts for all infrastructure?
- Who are the carriers in the mix?
- What is the current capacity (as contracted and as utilized)?
- How clean are the IPs?
- What are the security services offered?
- How frequently are systems patched?
Managed Services

Many organizations leverage third-parties to provide either on premise or remote managed services.

✓ What’s contracted in terms of SLAs, SLOs, and R&Rs?
✓ What’s being logged and for how long?
✓ What’s monitored and what are the responses?
✓ What happens when the contract expires?
✓ What are the core dependencies with the provider?
✓ Who are the provider’s material contractors / vendors?
✓ Are the provider’s vendors subject to the same controls and procedures?
Six (6) Key Vendor Management Lessons

1. Trust No One
2. Inspect What you Expect
3. Inventory Vendors Based on Risk Potential
4. Think out-of-the-box & leverage alternative, complementary disciplines
5. Vendor-Management is a Team Sport
6. Right-to-audit clause
Thank You

Matt Stamper – CISA, CIPP-US, ITIL
CISO in Residence
CyberFlow Analytics
mstamper@cyberflowanalytics.com
Matt.stamper.eag@gmail.com (Virtual CISO)
ISACA & COBIT
22 Vendor-Risk Mitigation Strategies

1. Diversify Sourcing
2. Establish Policies and Procedures for Vendor Management
3. Establish a Vendor Governance Model
4. Establish a Vendor Management Office
5. Establish Vendor Competencies & Skills Required
6. Use Standard Documents and Avoid Vendor-Supplied Documentation
7. Establish Clear Requirements
8. Perform Adequate Vendor Selection
ISACA & COBIT (continued)

22 Vendor-Risk Mitigation Strategies

9. Cover the full lifecycle with the contract
10. Define Security Practices & Controls
11. Establish SLAs and SLOs
12. Establish OLAs and underpinning agreements
13. Establish performance monitoring
14. Establish penalties and performance monitoring
15. Conduct vendor management during the life cycle
ISACA & COBIT (continued)
22 Vendor-Risk Mitigation Strategies

16. Review contracts and SLAs on a frequent basis
17. Conduct Vendor Risk Assessment
18. Perform evaluation based on policies
19. Evaluate vendor's internal controls
20. Plan and manage for the end of the vendor relationship
21. Use a vendor-management system
22. Create data and hardware disposal requirements