Collaboration with Business Associates on Compliance

HCCA Compliance Institute
April 19, 2016

Balancing risk management, compliance responsibility and business growth

Due Diligence and Satisfactory Assurance to Evaluate Business Risk
Vendor Management to Reduce or Eliminate Risk
Responsibility of entities as they engage one another in business activities

Co-Mingled Responsibilities of the Covered Entity and Business Associate

Privacy
- CE must comply with all requirements
- BA must comply with the requirements that pertain to the activities performed

Security
- CE must comply with all requirements
- BA must comply with 164.308, 164.310, 164.312, 164.314 and 164.316
Balance of Corporate Goals and Objectives and Compliance

When there is Conflict?

Compliance says “yes”!

Compliance Concerns

- Non-compliance can result in serious fines and legal action, leading to loss in investor confidence.
- The cost of compliance, though necessary, is not always seen as providing a return on investment.
- Effective compliance practices can be an asset to the organization, enhancing brand reputation.
- The evolution of regulations often requires updating compliance practices, adding complexity.
- New products or services require new compliance considerations, impacting overall strategy.

Compliance as an asset

- Effective compliance practices can serve as a competitive advantage during the sales process.
- Investment in compliance can equal opportunity costs.
- Reputation in a competitive market can drive the difference for growth opportunities.
- Non-compliance can lead to loss of market share, lost revenue, and inability to grow in a controlled market.
Control Review Team

Control Review Team - Compliance Review Team established for consistent monitoring and evaluation of policies, procedures and organization risk.
► Resolve conflict ensuring the adherence to corporate policy while reducing or eliminating risks for the organization.
► Ultimately the members of this team are the decision makers to determine when identified risk is acceptable risk and when decisions must be made to reduce or eliminate the risk that has been identified for existing or new operations.

Summary of Responsibilities

For all entities meeting the definition of a Covered Entity, Business Associate or Subcontractor general responsibilities we can all agree on would include:
► Protection of the confidentiality, integrity and availability of data;
► Ensure proper data security controls have been implemented appropriately;
► Obtain written satisfactory assurances (Business Associate Agreements);
► Prevention of fraud and abuse;
► Permitted and restricted uses and disclosures of PHI;
► Ensure PHI availability;
► Document policies and procedures;
► Training of staff, and as needed, business associates/subcontractors on Privacy, Security and Data Breach policies

Business Associate Agreements (written satisfactory assurances)

I. Outlines the responsibilities of the business associate and covered entity in the partnership they have created (receipt, creation, transmission, modification and storage) of data;
II. Defines the responsibilities to one another for notification, breach activity and security incidents that may put either organization at risk;
III. Details the acceptable practices for use and disclosure of PHI;
IV. Other addressed items in the agreements include, but is not limited to:
1. Language around where the financial burden resides;
2. Cyber insurance requirements and financial limitations;
3. Indemnification language;
4. Freedom to perform an audit;
5. PCI-DSS required language
Additional Satisfactory Assurances

What is the managing responsibility?
- Will none of a “second level” be appropriate?
- Is it going to be known by the risk?
- Will it be the main task (or not)?

Vendor Assessment

1. Define the process that will be used to evaluate a potential or existing business associate, vendor or subcontractor.
2. Develop a consistent method for risk determination.
3. Identify alternative solutions.
4. Determine how the final decision on risk acceptance will be made and who the final approver is.
5. Document the process, results and decisions that are made.

Pre-Contract Procedures

- Reputation or Reference Checks
  - Company History: How long have they been in business, industries or clients served, experience in the performance of the potential tasks;
  - References: Other clients or businesses they may have provided the same or similar service to;
- Security Risk Analysis
  - Due diligence to assess the risk of their systems, network, servers, transmission processes, storage of data etc.
- Evidence
  - Company’s certificate of insurance to ensure there is cyber protection;
  - Ensure the insurance is appropriate for the level of activities the company would be performing
  - Third Party Assessment - SOC2, PCI-DSS, HIPAA or equivalent security assessment
Pre-Contract Procedures, Cont...

- Risk Mitigation - Analyze the responses to the data security questionnaire to assess the level of risk to the organization and/or its customers/clients.
- Remediation plan for identified or known risks
- Pre-Contract Data Sharing - No data can be received, shared or transmitted without a formal written agreement.

Define the Process for Vendor Evaluation

<table>
<thead>
<tr>
<th>Functions Performed</th>
<th>Level of Data at Risk</th>
<th>Probability of Risk</th>
<th>Level of Assessment Needed</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor performs activities without access to critical data</td>
<td>Public Information</td>
<td>None</td>
<td>Not Required</td>
</tr>
<tr>
<td>Restricted access to internal documents only - no client data</td>
<td>Internet Use</td>
<td>Information accessed would not cause significant harm to the organization (polices, procedures). Excludes financial, PHI, PII or CC data.</td>
<td>Low-level assessment: Basic questions to determine if further risk assessment is necessary</td>
</tr>
<tr>
<td>Access to information</td>
<td>Confidential</td>
<td>Access to data that could cause harm to clients, the company or customers of our clients.</td>
<td>Mid-level assessment: High level questions related to security controls, data processes and training for Staff</td>
</tr>
<tr>
<td>Storage or Transmission of PHI/PII; support or maintenance of PHI/PII systems</td>
<td>Privacy Restricted</td>
<td>Data at risk for breach or public exposure which may cause harm (financial or reputation) to the organization or its clients.</td>
<td>High-level assessment: Detailed level of questions related to security controls, back-up processes, data processes and training of staff</td>
</tr>
</tbody>
</table>
## Determine Level of Assessment

Organize your assessment process:

<table>
<thead>
<tr>
<th>Name of the Vendor</th>
<th>Primary Function</th>
<th>Level of Vendor</th>
<th>Level of Data at Risk</th>
<th>Level of Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data 123 Storage</td>
<td>Data Center -</td>
<td>Primary</td>
<td>Privacy-Restricted;</td>
<td>High-level</td>
</tr>
<tr>
<td></td>
<td>Storage or</td>
<td></td>
<td>Critical (PHI/PII or</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transmission of</td>
<td></td>
<td>Card Holder Data)</td>
<td></td>
</tr>
<tr>
<td>DR 4U Disaster</td>
<td>Site</td>
<td>Primary</td>
<td>Privacy-Restricted;</td>
<td>High-level</td>
</tr>
<tr>
<td>ITSupport</td>
<td>Site</td>
<td>Primary</td>
<td>Critical (PHI/PII or</td>
<td>High-level</td>
</tr>
<tr>
<td></td>
<td>Site</td>
<td>Primary</td>
<td>Card Holder Data)</td>
<td></td>
</tr>
<tr>
<td>DeskTop</td>
<td>Computer installs;</td>
<td>Secondary</td>
<td>Confidential</td>
<td>Mid-level</td>
</tr>
<tr>
<td></td>
<td>workstation</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

## Assessment Categories

All level assessments can include the same topics, each level can determine how much detail the assessment should explore based on the severity of the risk the vendor may present to the organization. Topics typically covered in most assessments include:

- **General Company Information** - General demographics about the company's business including general description of the company, number of years in business, number of employees, address of additional locations.
- **Formal Compliance Programs** - Review of the formal process in place to manage compliance at an enterprise level, review existing policies and procedures for changes, evaluate company risk and determine compliance impacts to the organization. Performance of security risk analyses, third party reviews/assessments. Vulnerability management, frequency of scans, audits, most recent results of third party assessments (i.e., SOC2, HIPAA, PCI-DSS, GLBA). Assign responsibility for security.
- **Network Management** - Review the existence of wireless access, components of the network, a network diagram to ensure proper controls, firewalls, routers, switches have been properly protected to decrease the risk of a breach or security incident.
- **Breaches and Security Incidents** - Identify the number of incidents/breaches that have occurred and the general reason for such an event: Technical failure, human error, uncontrollable event or other causes. Incidents involving more than 500 people.
- **Access Control and Review** - Procedures for assigning access (role-based), reviewing and maintaining the authorized access, monitoring the access that has been granted, timeliness of access terminations, password strength requirements, frequency of password changes, and forced lock-outs.
- **Device Security** - Encryption and access controls for devices such as laptops, mobile devices, workstations, USB drives, servers, routers, and switches. Installation of firewalls, patches and updates for anti-virus malware protection. Storage of information on mobile devices (same device or alternative storage).
- **Physical and Environmental Security** - Perimeter security, camera locations, video tape availability, entry access (key, key fob, badge access), logs of the access, server room access, visitor procedures, escorted vendors and visitors, identification of equipment with privacy restricted data.
Assessment Categories

- **Data Storage**: Review the company’s back-up schedule, location of the back-up, time for retrieval, testing of failed back-ups, frequency of the back-up process. Data retention policies.
- **Disposal**: Review the disposal practices of the organization - on-site storage until the information is destroyed.
- **Audit and Monitoring Review**: Presence of internal monitoring and auditing of the organization’s business practices, compliance practices and security controls.

Assessment Level Descriptions

- **High-Level Assessment**: Vendors that put the organization at risk for data breaches, security incidents, public exposure, financial hardship or reputational damage. We want the assessment to identify such risks prior to the contract or as early as possible within a current relationship. The high-level assessment would be the deepest dive into each of the Assessment Categories.
- **Mid-Level Assessment**: The level of data at risk is confidential and could provide a risk to proprietary information, insider information that may cause harm to the reputation of the organization or cause or enable other harm to the organization. The mid-level assessment would focus on information that could result in data breaches or non-compliance fines.
- **Low-Level Assessment**: This level of an assessment is a basic due diligence that would identify whether or not a deeper level of an assessment would be necessary. Information at risk would be internal information such as policies, procedures, contracts, etc. that information would not generally include Confidential or Privacy Restricted data. There may be a few exceptions to this for example a Shredding Company.

Develop Consistent Method for Risk Determination
**Methods for Assessment**

- **Survey Format**
  - **Pros**
    - Topics that would provide space for a description of a process may reduce the number of questions that need to be asked in regards to that topic.
    - Allows the vendor to answer the questions based on their specific situation rather than selecting from a list of responses that may not apply to their business.
  - **Cons**
    - Variability in responses may make it difficult to compare one vendor to another.
    - Additional questions within a category that would be present in another format may provide a clearer picture and less to interpretation by the organization completing the form.
    - May slow down the responder since the majority of the responses will require a description versus yes/no or N/A.

- **On-line Tool**
  - **Pros**
    - Responses can be categorized and sorted to identify risks quickly.
    - Responses can be easily compared across multiple vendors.
    - Information received can be used to identify trends across all responders for review and modification of the assessment process.
    - Historical response information for each vendor can be reviewed for progress or outstanding problems.
    - Follow-up and mitigation documentation could easily be loaded in the same format.
  - **Cons**
    - Responses do not allow flexible answers when an answer doesn't quite fit.
    - Responders may guess at which answer most closely reflects their response when an available answer doesn't provide what is needed.
    - Responders may not be able to easily extract the questions and responses to disseminate to appropriate individuals for the proper information.
    - Might be more costly to create, purchase and implement.

- **Excel Workbook**
  - **Pros**
    - Marriage of the question/answer and on-line tool provides the standardization to the requestor but allows flexibility to the responder for the answers.
    - Excel expertise could provide to be an asset if the appropriate pivot tables, selections and gadgets of excel can be used to slice and dice information based on the function the vendor is performing on your behalf.
    - Vendors would only need to complete the sections that pertain to the activities they are performing for or on your behalf.
    - Most if not all businesses have the ability to open, modify and save in Excel.
  - **Cons**
    - Evaluation of the risk may require higher level of excel knowledge.
    - Development of the risk process may still be needed within excel do the data can be tracked and evaluated.
Evaluation of Risk

Risk status of a vendor may fall into the following categories:

<table>
<thead>
<tr>
<th>Critical Risk</th>
<th>High</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>A third-party risk analysis or security assessment has not been completed in more than two years.</td>
<td>Proof of acceptable third-party assessments were made available.</td>
<td></td>
</tr>
<tr>
<td>Risk posing a direct threat to data loss, theft, or breach has not been mitigated.</td>
<td>Minimal controls are in place to prevent a threat, loss, theft or breach.</td>
<td>Appropriate controls and monitoring in place to manage the risk.</td>
</tr>
<tr>
<td>Known security risks that create critical vulnerabilities to the organization's data.</td>
<td>Progress on mitigation but did not address critical items first.</td>
<td>Mitigation to known risks are handled promptly.</td>
</tr>
<tr>
<td>Supporting downstream assurances have not been conducted.</td>
<td>Downstream vendors do not have established compliance programs nor provide training.</td>
<td>Established compliance program with annual reviews.</td>
</tr>
<tr>
<td>Listed on the OCR with breach over 500 and vendor has not corrected the issue.</td>
<td>Policies and procedures are available but outdated.</td>
<td>Policies, procedures and training have been implemented.</td>
</tr>
</tbody>
</table>

Revisiting Organization Balance

Risk Acceptance

Acceptable Risk

Unacceptable Risk
Remediation and/or Alternative Solutions

What do you do when risk has been identified?

1. Obtain the corrected or remediated vendor documentation (policies, procedures, implementation plan, screen shots for proof of activity or any other documentation that may be necessary to remediate or prove remediation has been completed).
2. Schedule follow-up meetings with the subcontractor/vendor to ensure progress of the mitigation plan and documentation has been received.
3. Document the acceptable and unacceptable mitigation risks and determine whether or not the subcontractor/vendor can be kept or needs to be replaced.
4. Propose recommendations to the Control Review Team for the continuance or termination of the vendor for decision if remediation cannot be obtained; and/or
5. Follow up with the vendor until all remediation has been completed.

Final Decision

1. Determine the criteria that will make the decision a "go" or "no go" decision.
2. Develop a process for resolving conflict.
3. Identify the steps that will be needed to support a decision to move forward with a vendor that may bring additional risks to the organization.
4. Report the progress to the Executive Team as the remediation occurs.
Contact Slide

Christine Duprey, Caris Consulting, LLC
2951 Sunray Lane,
Green Bay, WI 54313
(920) 639-6615
chris@carisinnovation.com
www.carisinnovation.com