Third party vendor management

Bank of America Merrill Lynch

Use strong vendor management to help reduce fraud risk:

As businesses evolve, many organizations are using third party vendors to achieve their strategic objectives. Whether it's to increase efficiency or reduce costs by shifting non-core or specialized functions to experienced providers, businesses must be sure strong controls and monitoring strategies are established. Vendor fraud is on the rise and fraudsters know that many companies do not have the proper vendor controls in place to mitigate their fraud risk.

Vendor management lifecycle

Vendors hold key information about your company, such as key contacts, associate roles, payment information and purchase details. Ensuring your vendor is keeping confidential information secure is essential during the vendor lifecycle.

Vendor identification and planning: Prior to engaging vendors, organizations should incorporate the following elements into the vendor vetting process:

- Business cases: Develop business cases that consider risk, expected performance, risk management outcomes and costs associated with managing, monitoring and testing the vendor.
- Compliance: Require compliance input and approval to be sure regulatory impacts are appropriately reflected in business cases.
- Contingency Operations: Engage with contingency and continuity teams to properly vet vendor contingency plans and controls.

Vendor risk segmentation[1]

Each vendor relationship is unique and poses a different level of risk. Organizations should conduct a vendor risk segmentation and assess whether or not a vendor has access to confidential data or is considered mission critical. Vendors should be categorized in the following segments to allow for an initial risk assessment to build a cascading model of oversight.

- **Tier one - high risk:** This segment encompasses vendors that provide critical services, have access to sensitive or proprietary information or provide a specific concentration of services.
- **Tier two - moderate risk:** This segment encompasses vendors that use used frequently but are not "mission critical" to an organizations operational functionality. Vendors in the segment typically have access to sensitive or proprietary information.
- **Tier three - low risk:** This segment includes non-critical vendors who do not pose a data or direct consumer risk.

Vendor Sourcing

After an organization has conducted the proper vendor identification, planning and risk segmentation organizations should start the sourcing phase.

- **Due Diligence:** Organizations should conduct comprehensive due diligence to be sure a vendor's ability and willingness to meet business performance and risk management expectations.
- **Laws, rules and regulations:** Require adherence to all laws, rules and regulations that impact the organization or vendor relationship. Engage with internal legal, risk and compliance departments to be sure standards are met.
- **Vendor selection:** Select the vendor best suited to meet your organization's needs. Be sure the vendor contract specially states service level

[1] http://www.mortgagecompliancemagazine.com/vendor-management/effective-vendor-management-best-form-risk-management/

agreements and risk management requirements identified in plan.

Vendor Management

Once the vendor is fully on-boarded proper management of the vendor relationship is essential in order to meet business objectives.

- **Monitoring activity:** Monitor vendor activity and management routines to identify risk and assess vendor performance. Emphasis should be placed on adherence with applicable laws, rules, policies and standards.
- **Metrics and Scorecards:** Utilize vendor scorecards and metrics to monitor vendor performance and adherence to laws, rules and regulations.
- **Issue identification:** When issues are identified document, escalate and work with vendor to be sure proper remediation.
- **Incident Response Plan:** Incident response plans should capture third party vulnerabilities as well as steps to mitigate or respond to a breach. Tabletop exercises should be utilized to simulate potential third party breaches and response plans.

Addressing problems and relationship termination

- **Prompt action:** It is essential to take prompt action if a vendor is found to be out of compliance. Organizations should have protocol in place to address a concern with a vendor. It's a best practice to require a written response from the vendor to document their file. Remediation may also be required especially when dealing with a cybersecurity or data breach.
- **Update policies and procedures:** If a vendor is found to be out of compliance organizations should require vendors to update their policies and procedures to close any identified gaps or to mitigate the chance of encountering noncompliance in the future.
- **Termination:** If all attempts at mitigating vendor non-compliance fail it may be necessary to terminate the vendor relationship. This is why having a written back-up plan for "mission critical" vendors is essential.

Vendor Best Practices

Vendors that handle payment and financial transaction information for organizations are especially vulnerable to cybercriminals. Below are some best practices for managing accounts payable vendors.

Vendor best practices

- **Access controls:** Be sure users are only provisioned the minimum access required to complete their assigned role. Be sure key security principles such as least and separation of privilege are enforced without exception.[2]
- **Request for proposal:** When vetting a potential new vendor, leverage security experts within your company to evaluate capabilities. Performing site visits and security reviews can help to be sure that the vendor has similar security standards. Security can be your organizations competitive differentiator. Vendors should have the same holistic approach to security and data protection as your organization.
- **Vendor master file:** When adding a new company to a vendor master file proper vetting can help reduce exposing your organization to compliance risks. Be sure that duplicate or expired entries are scrubbed from your organizations master list. Implement a robust vendor registration process to help prevent fraud. Employ continuous monitoring techniques to be sure that the master list contains valid up to date information.
- **Be sure Vendor Security:** Vendors should utilize appropriate data protection security, safeguards and appropriate intrusion detection. If confidential or proprietary information is exposed employees may be targeted with phishing emails which could possibly open an organizations system to unauthorized access.

[2]https://www.csoonline.com/article/3251714/authentication/what-is-access-control-5-enforcement-challenges-security-professionals-need-to-know.html

- **Always hold vendors to your organizations own internal security standards:** Leverage the security experts within your company or an external cyber security firm to evaluate the security capabilities of your vendors. Perform site visits and confirm security review tests. Always limit vendor logins and access to your organizations data and systems. Only give vendors access to what is absolutely necessary to conduct contractual work.

- **Always remember information security is a competitive differentiator:** When evaluating a vendor relationship be sure that their security protocols are in alignment with your own organizations standards. Evaluate vendors on who has the best security program and be sure that their policies and controls are auditable and similar to your own.

Data Security

Data for many organizations is their competitive differentiator and as such is at risk for cybercrime and espionage. Even for organizations that don't competitively utilize stored data, clients expect effective controls and confidentiality of trusted data. Organizations should maintain a holistic view of their data and utilize the following framework to view data.

- Data is Valuable: as the volume of data increases so does an organization vulnerability to cyber-attacks. Data is not only valuable to organizations but it is bought and sold on the black market for illicit purposes.
- Maintain strong controls and know who has access to your data: It's essential for organizations to know who has access to their data and what level access. Only allow users to access data that have a need to know as outlined by their role and job description. Be sure vendors are held to the least privilege standard and never allow open access to organizational data.
- Archive and store data securely: proper storage is essential to data security. There are many data storage options whichever one your organization decides to utilize be sure that you know how it's stored and where it's located.
- Create a strong data protection policy: always know who is protecting your data and what security processes are in place. In the event of a breach establish and implement an incident response plan.

For more information

For more information about vendor management, visit our Fraud Education site through CashPro Assistant at: http://cashprouniversity-dev.bankofamerica.com/cpocms/sites/CashProUniversity/Landing/Fraud/page.htm