VENDOR MANAGEMENT

General Overview

With many organizations outsourcing services to other third-party entities, the issue of vendor management has become a noted topic in today’s business world. Vendor management principles have been around for many years as common due diligence practices constituted a normal part of business for any entity relying on another for services. The banking community has utilized vendor management principles for many years, as the FDIC Compliance Examination Manual states that,

“The board of directors and senior management of an insured depository institution (institution) are ultimately responsible for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution.”

-Source: fdic.gov

Proper vendor management means conducting extensive due diligence in vendor selection, assessing current vendors with regards to minimum requirements, reviewing all necessary contractual documentation, along with numerous continuous monitoring activities and management oversight. What’s brought about increased focus on vendor management is the growth in information technology and the need for properly monitoring an organization’s growing list of third-party providers. Using the baseline parameters for vendor management developed by the banking industry, while also including provisions relating to information technology, results in a comprehensive vendor management policy and procedures document listed below.

Vendor Management Policy and Procedures

1.0 Overview

In accordance with mandated organizational security requirements set forth and approved by management, [company name] has established a formal Vendor Management policy and supporting procedures. This policy is to be implemented immediately along with all relevant and applicable procedures. Additionally, this policy is to be evaluated on a(n) [annual, semi-annual, quarterly] basis for ensuring its adequacy and relevancy regarding [company name]'s needs and goals.

1.0 Purpose

This policy and supporting procedures are designed to provide [company name] with a documented and formalized Vendor Management policy that is to be adhered to and utilized throughout the organization at all times. Compliance with the stated policy and supporting procedures helps ensure the safety and security of [company name] system resources.

Today's increased use of outsourcing to various third-parties has created a true need for monitoring such entities for baseline compliance measures with regards to [company name]'s minimally accepted standards for security. Specifically, all outsourced processes, procedures, and practices relevant to [company name]'s business are to be monitored on a regular basis, which includes undertaking various measures on all third-parties providing critical services. The subsequent policies and procedures relating to vendor management initiatives for [company name] strive to ensure the overall confidentiality, integrity, and availability (CIA) of the organization's network.

1.0 Scope

This policy and supporting procedures encompasses all system resources that are owned, operated, maintained, and controlled by [company name] and all other system resources, both internally and externally, that interact with these systems.

- Internal system resources are those owned, operated, maintained, and controlled by [company name] and include all network devices (firewalls, routers, switches, load balancers, other network devices), servers (both physical and virtual servers, along with the operating systems and applications that reside on them) and any other system resources deemed in scope.

- External system resources are those owned, operated, maintained, and controlled by any entity other than [company name], but for which these very resources may impact the confidentiality, integrity, and availability (CIA) and overall security of the aforementioned description of "Internal system resources".

- When referencing the term "users", this includes any individual that has been granted access rights by [company name] to various system resources and has went through all required provisioning steps. Users typically include, but may not be limited to, the following: employees, consultants, vendors, contractors, along with local, state, and federal personnel.

- For purpose of this policy, vendor management is defined as the following: The policies, procedures and related processes undertaken for managing activities conducted through third-party relationships, and identifying and controlling the risks arising from such relationships, to the same extent as if the activity were handled within the institution.

- Additionally, the terms “vendors”, “third-party”, third-parties”, “outsourcers”, “organizations”, and an variant thereof are defined as entities providing outsourcing services to [company name].

1.0 Policy

[Company name] is to ensure that the vendor management policy adheres to the following conditions for purposes of complying with the mandated organizational security requirements set forth and approved by management:

Elements of Risk

When using the services of various third-party outsourcing entities, a certain element of risk arises as responsibilities for critical initiatives are now in the hands of another organization. It’s important to understand these risks, what they are, and how [company name] can readily identify any issues, concerns, or constraints pertaining to these risks. Failure to mitigate and prevent these risks can result in significant financial loss, legal issues, and public opinion misconceptions, ultimately damaging the organization. As such, the following risks are to be thoroughly understood and assessed in regards to business and contractual relationships entered into with various third-parties:

- **Compliance Risk:** These are risks arising from violations of applicable laws, rules, regulatory mandates, and along with other issues, such as non-compliance of internal operational, business specific, and information security policies, procedures, and processes. A common example would be for an outsourced organization to violate compliance regarding the safety and security of Personally Identifiable Information (PII), such as having exposed such information to unauthorized parties, not having policies and procedures in place protecting PII, or not undergoing required annual compliance audits (i.e., SSAE 16, etc). Regulatory compliance is a large and critically important component for vendor management, requiring constant monitoring and oversight of third-parties for ultimately ensuring the safety and security of services being provided to [company name] by such entities. Common compliance initiatives for which third-parties are to adhere to including numerous laws, legislative mandates, and industry specific requirement, including, but not limited to, the following: Sarbanes-Oxley, HIPAA, HITECH, SOC 1 SSAE 16, SOC 2 and SOC 3 AT 101, GLBA, PCI DSS, and many others.

- **Reputation Risk:** These are risks arising from negative public perception and opinion of a third-party outsourcing entity for almost any imaginable reason, such as unethical business practices, data breaches resulting in loss of sensitive and confidential consumer information (i.e., Personally Identifiable Information - PII), investigations from regulators into questionable business practices, etc. It’s important to note that in today’s world of transparency and close media scrutiny, any perceived negative public opinion on a third party being utilized by [company name] ultimately affects the reputation of this organization. The rise of social media and many non-traditional media outlets have the ability to spread a story, going “viral” in literally minutes.

- **Strategic Risk:** These are risks arising from third-parties failing to implement business initiatives that align with the overall goals and ideas of [company name], such as not offering services that provide an acceptable return on investment, both short term and long term. Ultimately, when the long term strategic vision of both [company name] and the applicable third-party outsourcing entities do not align, relevant risks begin to surface which can significantly impact the business relationship, often in a negative manner.

- **Operational Risk:** These are risks arising from a failed system of operational internal controls relating to personal and the relevant policies, procedures, processes, and practices. This becomes a large issue due to the fact the many organizations integrate their daily operational activities with outsourcing providers, thus a "breakdown" on the vendor side seriously impacts the organization, ultimately affecting productivity, workflow efficiency, and many other issues.

- **Transaction Risk:** These are risks arising from a third-party failing to deliver as promised, such as product delivery, operational efficiency - or worse - unauthorized transactions and theft of information due to a weak system of operational and information security internal controls. An important component of mitigating such risks is having comprehensive, well-documented operational and information security policies, procedure, processes, and practices in place for guiding such third-parties on a daily basis.

- **Credit Risk:** These are risks arising from the financial condition of the third-party, such as any "going concern" issues - a business that functions without the threat of liquidation for the foreseeable future, usually regarded as at least within 12 months. Not being able to meet routine expenses can result in large risks for [company name] as the organization is heavily dependent on various outsourcing entities for their services. A ceasing of operations because of credit risks can seriously impact [company name] in many ways.

- **Country Risk:** These are risks arriving from the politic, economic, and social landscape - and other relevant events - within a foreign country that can impact the services being provided by the third - party, ultimately affecting operations for [company name]. Managing such risks can be extremely challenging and complex, especially when one considers the diverse political landscape in various regions around the globe. Legal issues also can pose significant country risks, as laws and regulations differ greatly from region to region.

- **Information Technology Risk:** These are risks arising from any number of information technology and information security issues, such as inadequate I.T. resources (hardware and software) along with lack of manpower. Additionally, risks can arise from abuse, misuse of information technology resources, while data breaches and security compromises can occur because of improperly designed networks, little to no information security policies, procedures, etc. Other serious information technology risks can include not correctly provisioning and hardening critical system resources, failing to implement "defense in depth" and layered security protocols, etc.

Benefits of Vendor Management

True vendor management is much more than just meeting regulatory compliance purposes - while though extremely important - many other considerations are to be looked upon. Specifically, vendor management initiatives for [company name] should seek to help reduce costs, improve operations, strengthen security, while also improving relationships with all applicable third-party outsourcing entities. Vendors for [company name] are looked upon as instrumental organizations providing critical services, and as such, are to be taken seriously in every manner, which means assessing all aforementioned risk areas, while also striving for the following:

- **Reduction of Costs:** Cost-containment, while not the only qualifier for vendor selection, is extremely important, requiring [company name] to thoroughly assess new and upcoming contracts with all applicable parties. Furthermore, issues such as automatic renewals and other automated binding agreements are to identified well in advance (90 to 180 days at a minimum) of any contracts coming up for renewal. Fair and equitable leverage points are to be utilized at all times for maximizing services for new and additional contracts. Additionally, requests for proposals (RFPs) are to be announced for ensuring competitive price bids on all services for [company name].

- **Improvement of Operations:** Vendors, no matter how material and significant to [company name]'s operations, still function independently and are generally located in different geographical areas. For these reasons alone, it's important to undertake regular operational assessments for performance and efficiency, such as receiving daily, weekly, monthly performance metrics, physical site inspections, and other initial and on-going operational due diligence practices. This information is extremely valuable for helping assess operational capacity and performance issues, helping to identity any areas of weakness requiring remediation, etc.

- **Strengthening of Security:** [Company name] can learn from vendors, just as they can learn from us, and in many areas relating to operations, performance, etc. A key area is information security - policies, procedures, and practices for ensuring the confidentiality, integrity, and availability (CIA) of [company name]'s overall information systems landscape. Sharing of security protocols and measures is critical, especially in today's world of growing cyber security threats and malicious attacks. Both [company name] and all applicable third-party outsourcing organizations are to have formalized information security policies and procedures in place and specifically for areas relating to incident management, security awareness, business continuity and disaster recovery planning (BCDRP) and other important measures. The use of technology continues to grow at a rapid pace, ultimately demanding strong collaboration amongst [company name] and all third-parties.

- **Improvement of relations:** Communication is the primary ingredient for successful relationships with all third-parties providing services to [company name]. The more [company name] communicates, asks intelligent and thoughtful questions, the stronger the relationship is with such third parties, ultimately improving relations. Asking the tough and necessary questions, resolving disputes in a timely manner and being aware of issues, constraints and concerns on both sides, resulting in strong relationships between [company name] and third-parties, ultimately improving performance, reducing costs, etc.

Current Vendor Assessment Analysis

True vendor management also entails assessing one's current list of third-party outsourcing organizations, while also putting in place initiatives for evaluating new vendors - and finally - implementing continuous monitoring practices. Specifically, [company name]'s current vendor assessment analysis are to comprehensively assess each organization in regards to the aforementioned risks areas, which include, but are not limited to, the following:

- Identify all third-party outsourcing organizations.
- Obtain all contractual documents and other supporting documentation for helping assess current third-party services. This may also include legal correspondence, audited financial statements, various expenses and revenues directly tied to such providers, etc.
- Obtain all regulatory compliance reports. This may include assessment such as SOC 1 SSAE 16, SOC 2 AT 101, PCI DSS, FISMA, ISO, and many other compliance mandates and reports.
- Identify, review, and assess any consumer complaints, unethical business practices, etc.
- Identify, review, and assess any data security breaches, cyber security attacks, etc.
- Identify if any third-parties are storing, processing, and/or transmitting any sensitive and confidential information, commonly known as Personally Identifiable Information (PII) and any derivative thereof.
- Identify, review and asses all operational, business specific, and information security policies, procedures, and practices relevant to services being provided to [company name], particularly documentation pertaining to incident response, security awareness, business continuity and disaster recovery planning (BCDRP).
- Identify review, and assess all information technology platforms (hardware and software) and I.T. personnel relevant to services being provided to [company name], particularly what systems are being used, and the skill sets and experience of these individuals.
- All other measures deemed necessary by [company name].

Due Diligence in Vendor Selection

The selection process for new vendors is to consist of exhaustive measures for ensuring all relevant aforementioned risk areas have been thoroughly assessed by [company name], which is to include, but not limited to, the following measures:

- Review of all applicable financial documentation, such as financial statements, etc.
- Review of all regulatory compliance and operational audits and assessments, etc.
- Experience and overall business "know-how".
- Operational capacity and scalability.
- Use of other third-parties by the actual vendors themselves (i.e., sub servicers, etc.)
- Reputation within the industry and from the general public.
- Inquiry into any past, present or expected legal issues, constraints, or concerns.
- Experience and business aptitude, strength, and knowledge of senior management and all other relevant personnel.
- Alignment of vision, strategies, and overall goals with each organization

- Assessment of operational, business specific, and information security policies, procedures, and practices, particularly documentation pertaining to incident response, security awareness, business continuity and disaster recovery planning (BCDRP)'
- Assessment of organizational-wide system of internal controls.
- Underwriting criteria
- Insurance coverage

Contractual Documentation

Once vendors have been selected for providing critical outsourcing services to [company name], comprehensive procedures are to be undertaken regarding all contractual documentation - specifically - the following:

- A formalized and written contract has been produced, one that dutifully identifies roles, responsibilities, obligations, and expectations from all relevant parties.
- The contract has been approved by senior management throughout [company name], which includes all major stakeholders, such as board of directors, audit committee personnel, equity owners, officers, - as applicable - and all other relevant personnel. This also requires addressing the following issues regarding stakeholders:
  - Are they aware of the risks when entering contractual agreements with such vendors?
  - Are there any financial relationships or associations with such vendors?
  - Were all due diligence findings and documentation presented clearly and in a timely manner to such individuals?
- Comprehensive and appropriate review undertaken by legal-council, with all issues, constraints, and concerns addressed as necessary.
- Defined operational, performance, and other necessary baseline standards for services to be performed, along with reporting metrics on such issues, such as daily, weekly, and monthly reports.
- Fees paid for stated services along with other financial considerations.
- Regulatory compliance audits and mandates, such as annual financial statement audits, annual operational and security assessments (i.e., SOC 1 SSAE 16, SOC 2 | SOC 3 AT 101, PCI DSS, etc.).
- Information security protection measures regarding the safety and security of sensitive and confidential information, such as Personally Identifiable Information (PII), and any other variant thereof.
- Numerous other legal issues, including, but not limited to, the following: resolution measures, indemnification, continuation of services, default, intellectual property

Management Oversight and Continuous Monitoring

Upon successfully approving all business agreements with vendors, management of [company name] is to continuously monitor the various aspects of the outsourcing entity as it relates to compliance risk, reputation risk, strategic risk, operational risk, transaction risk, credit risk, country risk, information technology risk. A large part of continuous monitoring involves significant input from senior management - personnel directly responsible for the long-term strategic vision of [company name] - thus policies, procedures, and practices are to be reviewed and approved by such individuals for ensuring a strong working relationship with all vendors providing critical outsourcing services. One of the largest areas for risk involves information security - specifically - ensuring that all vendors have well-documented, formalized policies and procedures in place along while adhering to I.T. best practices in today's world of growing cybersecurity threats and malicious exploits. The subsequent checklists include comprehensive due diligence and continuous monitoring practices to be undertaken by [company name] when working with new, current, or prospective vendors seeking to provide critical outsourcing services.

1.0 Additional Supporting Information and Documentation

This section is provided to you for the purposes of adding any additional comments or information that you feel are relevant to this specific policy document. Suggestions would include listing any existing policies, procedures, processes, and other supporting documentation (forms, checklists, etc.) that you may have in place along with commenting on any modifications or omissions you have made to this specific section.

1.0 Responsibility for Policy Maintenance

The [title of responsible party] is responsible for ensuring that the aforementioned policy is kept current as needed for purposes of compliance with mandated organizational security requirements set forth and approved by management.

Current Vendor Assessment Analysis Checklist

Procedure	Responsible Party	General Notes | Comments
Identify all third-party outsourcing organizations.		
Obtain all contractual documents and other supporting documentation for helping assess current third-party services. This may also include legal correspondence, audited financial statements, various expenses and revenues directly tied to such providers, etc.		
Obtain all regulatory compliance reports. This may include assessment such as SOC 1 SSAE 16, SOC 2 AT 101, PCI DSS, FISMA, ISO, and many other compliance mandates and reports.		
Identify, review, and assess any consumer complaints, unethical business practices, etc.		
Identify, review, and assess any data security breaches, cybersecurity attacks, etc.		
Identify if any third-parties are storing, processing, and/or transmitting any sensitive and confidential information, commonly known as Personally Identifiable Information (PII) and any derivative thereof.		
Identify, review and asses all operational, business specific, and information security policies, procedures, and practices relevant to services being provided to [company name], particularly documentation pertaining to incident response, security awareness, business continuity and disaster recovery planning (BCDRP).		
Identify review, and assess all information technology platforms (hardware and software) and I.T. personnel relevant to services being		