SAI360

RISK FROM EVERY ANGLE

Vendor Risk Management

Table of Contents

Introduction

In today's business environment, almost all firms rely on a network of vendors to provide essential services. This growing reliance on third-party service providers[1] is a phenomenon that affects various industries and sectors, including the financial sector. Third-party service providers are entities that perform a process, service or activity on behalf of a firm which the firm would otherwise carry out itself. For example, a firm can outsource the hosting of a data center or a business process to a third party.

One of the main drivers of this trend is the increasing complexity and interdependency of business operations, which require specialized skills and technologies that may not be available or cost-effective within the firm. By outsourcing some functions to third parties, firms can benefit from economies of scale, innovation, flexibility and efficiency.

However, this growing reliance on third parties comes with increased risk.[2] Adversaries are turning their focus towards cheaper, easier pathways to an organization, and often the weak link can be a third party. This is especially so as businesses increasingly rely on software and technology, which is invariably sourced from a vendor. Firms have an increasing dependence on third-party providers, vendors, service providers, and outsource partners.

This increased dependency leads to an increased vulnerability and means firms need to effectively manage the risks they pose of operational disruption and harm to their consumers. As such, the importance and growth of third-party ecosystems cannot be overstated.[3] With the expanding interconnectedness of businesses, it's more crucial than ever for organizations to think beyond just third parties and focus on mapping out their entire vendor ecosystem.[4] This involves being aware of their vendors' vendors, and in some cases, even further down the supply chain.

[1] https://www2.deloitte.com/content/dam/Deloitte/no/Documents/risk/Current%20trends%20in%20outsourcing%20and%20addressing%20third%20party%20risk.pdf

[2] https://www2.deloitte.com/content/dam/Deloitte/uk/Documents/audit/deloitte-uk-third-party-gov-risk-management-2016.pdf

[3] KPMG 2020 CEO Outlook: COVID-19 Special Edition

[4] Third Party Risk Management outlook 2020 (kpmg.com)

Risk to Reward

There are numerous benefits and risks associated with relying on third-party vendors. To make informed decisions and manage these risks, organizations must carefully weigh the potential rewards against the inherent risks:

Benefits

- **Specialized skills and expertise**: Third-party vendors often possess specialized knowledge, skills, and expertise that might not be available in-house. By outsourcing certain functions, firms can access these valuable resources to rapidly improve their operations.
- **Reduced operational costs**: Outsourcing non-core functions can result in significant cost savings for organizations.[5] Third-party vendors can provide these services more efficiently due to economies of scale, which in turn can help reduce operational costs.
- **Increased flexibility and scalability**: Utilizing third-party vendors allows organizations to quickly scale up or down as needed, providing greater flexibility to adapt to changing market conditions and business requirements.
- **Innovation and competitiveness**: Outsourcing can enable organizations to leverage best practices and cutting-edge technologies offered by third-party vendors, which can drive innovation and increase competitiveness. Otherwise, the use of innovative third-party technologies gives firms instant access to the latest breakthroughs without the need to develop them internally.

Risks

Outsourcing can create more potential entry points for criminals, such as technological vulnerabilities exploited in cyber-attacks. This increased 'attack surface' is not only a vulnerability with respect to criminals, but to simple human or system error, too. If a cybersecurity breach occurs through the vendor, the host company's information is also at risk. And the greater the dependency, the higher likelihood of major disruption or data loss should such a breach occur.

Beyond cyber risks, there are various other operational risks associated with outsourcing. If a vendor fails to meet their Service Level Agreements (SLAs), it can result in disruptions to the firm's operations, affecting efficiency and potentially causing financial losses. Additionally, reputational risk arises if a service provider's behavior is not up to par, potentially tarnishing the firm's image in the eyes of its customers and stakeholders. Legal risks also come into play if a vendor engages in activities such as anti-bribery/corruption, modern slavery, or other violations while providing services on behalf of the firm. These risks can lead to regulatory penalties, lawsuits, and further reputational damage, emphasizing the importance of thorough vendor risk management (VRM).

[5] ISO - Outsourcing's booming business

What are regulators saying?

The growing interdependence between firms and third parties has caught the attention of global regulators. They require that firms approach third-party relationships and controls with the same level of rigor that they apply to their own operations. Regulations in the U.S. are often fragmented and sector specific. This section provides an overview.

Federal Reserve Guidance on Managing Outsourcing Risk

The Federal Reserve has issued Guidance on Managing Outsourcing Risk[6] to assist financial institutions in understanding and managing the risks associated with outsourcing a bank activity to a service provider. The guidance describes the characteristics, governance, and operational effectiveness of a financial institution's service provider risk management program for outsourced activities. The guidance specifies various actions and their outcomes.

WHEN ACQUIRING A THIRD-PARTY SERVICE, FIRMS SHOULD:

- Conduct a thorough risk assessment to identify potential risks associated with the outsourced activity
- Perform due diligence on the service provider to evaluate their qualifications, reputation, and financial stability
- Review contract provisions to ensure that they clearly define the rights and responsibilities of each party
- Establish an effective oversight and monitoring program to ensure that the service provider is meeting performance standards and complying with applicable laws and regulations
- Account for business continuity and contingency planning to ensure that critical services can be maintained in the event of a disruption

[6] https://www.dataguidance.com/opinion/usa-federal-reserve-guidance-managing-outsourcing

The Gramm-Leach-Bliley Act (GLBA)

The Gramm-Leach-Bliley Act[7] (GLBA) is a U.S. federal law that regulates the information-sharing practices and data security measures of financial institutions. The GLBA aims to protect the privacy and security of consumers' non-public personal information (NPI) that is collected, used, or shared by financial institutions. The GLBA has three main rules that affect financial institutions' outsourcing activities:

The Privacy Rule

Requires financial institutions to provide customers with a notice of their privacy policies and practices, and to allow customers to opt out of sharing their NPI with unaffiliated third parties.

The Safeguards Rule

Requires financial institutions to develop, implement, and maintain a comprehensive information security program that includes administrative, technical, and physical safeguards to protect customer information from unauthorized access, use, or disclosure. The use of third parties will extend the scope of these security programs.

The Pretexting Rule

Prohibits financial institutions from obtaining customer information from third parties by false or fraudulent means, such as impersonating a customer or using deceptive tactics.

The Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act[8] (HIPAA) is a federal law that sets national standards for the protection of sensitive patient health information from unauthorized disclosure or use. The HIPAA Privacy Rule and the HIPAA Security Rule establish the requirements for covered entities and their third party service providers to safeguard this information, known as protected health information (PHI).

When outsourcing a health-related activity to a service provider, covered entities should consider the following:

- **Risk analysis:** Identify the potential threats and vulnerabilities to the confidentiality, integrity, and availability of PHI
- **Risk management:** Establish adequate security, based on what's learned during the risk analysis, to mitigate risks and vulnerabilities to an acceptable and suitable degree in accordance with the HIPAA Security Standards
- **Information system activity review:** Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports
- **Response and reporting:** Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or third party; and document security incidents and their outcomes

[7] https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
[8] https://www.cdc.gov/phlp/publications/topic/hipaa.html

The Sarbanes-Oxley Act (SOX)

The Sarbanes-Oxley Act (SOX)[9] is a U.S. federal law that was enacted in 2002 to protect investors from fraudulent accounting and financial practices by publicly traded companies. The law was a response to several corporate scandals, such as Enron and WorldCom, that resulted in huge losses for investors and damaged public trust in the financial markets. SOX requires companies to establish and maintain effective internal controls over their financial reporting and disclosure processes. These controls are designed to ensure the accuracy, reliability, and timeliness of financial information, as well as compliance with applicable laws and regulations.

Vendor risk management is a key area of firms' internal controls, covering the processes of identifying, assessing, and mitigating the risks associated with outsourcing a business activity to a third-party service provider. Vendor risk management is essential for SOX compliance since outsourcing does not transfer the responsibility or accountability for the outsourced activity from the company to the vendor. The company remains liable for any errors, omissions, or fraud committed by the vendor that affect its financial reporting or disclosure.

The Payment Card Industry Data Security Standard (PCI DSS)

The Payment Card Industry Data Security Standard (PCI DSS)[10] is a global standard that provides a baseline of technical and operational requirements designed to protect account data from major card brands. PCI DSS requires that organizations implement security measures such as encryption, firewalls, access control, vulnerability scanning, penetration testing, and incident response. Under PCI DSS, merchants must implement third-party risk management programs to oversee and monitor vendors and service providers handling sensitive card information. And, in accordance with PCI DSS guidelines, vendors themselves must be held to compliance with payment security standards.

[9] https://sarbanes-oxley-act.com/

[10] https://www.pcisecuritystandards.org/document_library/?document=pci_dss

Future-proof your VRM framework

Vendor Risk Management (VRM) is the process of identifying, assessing, and mitigating the risks associated with outsourcing services or products to third parties. VRM is essential for ensuring that vendors meet the contractual obligations, service level agreements, and compliance requirements of the wider group / organization.

Firms must have an overarching vendor risk management policy which sets out how it will identify material service providers and manage the arrangements with such providers, including the management of material risks associated with the arrangements. This policy will be operationalized through a VRM framework which, taking into account all aforementioned regulatory obligations, should look something like this:

- **Vendor Due Diligence:** Before entering into service agreements, it is important that the organization performs due diligence checks on potential vendors to evaluate their financial stability, reputation, performance history, security posture and compliance status. The organization should also define the scope of work, expectations, and responsibilities for each vendor off the back of this risk assessment.

- **Vendor mapping / identification:** The organization should identify and maintain a register of its current material service providers. Material service providers are those on which the entity relies to undertake a critical operation or that expose it to material operational risk. Examples might include risk management, core technology services, internal audit, credit assessment, and payments service providers.

- **Vendor risk assessment:** The organization should conduct risk analysis and assessment to identify the sources, likelihood, and impact of vendor-related risks.

- **Risk mitigation / controls:** The organization should implement appropriate controls and measures to prevent or reduce the impact of any potential risks or threats that may arise from the vendor relationship. The organization should also develop contingency plans and backup strategies to ensure business continuity and resilience in case of vendor failure or disruption.

- **Ongoing monitoring:** The organization should also track and measure the vendor's performance and compliance against the contract and the organization's policies and standards. This involves establishing key performance indicators (KPIs), service level objectives (SLOs), and metrics to evaluate the vendor's service quality, availability, reliability, and security. The organization should also conduct regular audits, reviews, and assessments to verify the vendor's adherence to the regulatory requirements.

Supercharge your VRM with technology

Leveraging technology can significantly enhance your VRM efforts by reducing operational costs, improving compliance, and enabling your organization to scale securely and efficiently. Technology is not only a driver of efficiency, through automation, but also of insight and assurance based on its ability to collect and analyze more data, more frequently. Further, advanced analytical techniques and visualizations help to maximize insight from the data available.

Here are five noteworthy applications of technology in VRM:

1. **Risk-based assessments**: Utilize configurable questionnaires, industry standard frameworks, and workflows to conduct risk-based assessments of your vendors. This will help streamline the evaluation process and ensure that you're focusing on the most critical risk factors associated with each vendor.

2. **Real-time monitoring**: Use real-time data feeds, alerts, and dashboards to continuously monitor vendor risks. This approach enables you to stay informed of any emerging risks or issues and take timely, proactive measures to mitigate potential threats.

3. **Centralized issue and incident management**: Implement a centralized repository and remediation tools to manage vendor issues and incidents. This allows for better tracking, coordination, and resolution of issues while promoting transparency and accountability within your organization.

4. **Performance evaluation**: Establish key performance indicators and scorecards to evaluate vendor performance against predefined benchmarks. This process ensures that vendors are meeting the expected service quality, availability, reliability, and security standards.

5. **Advanced reporting and analytics**: Incorporate advanced analytics and visualization tools to generate insightful reports on your vendors' performance and compliance. These reports can help you identify trends, patterns, and areas for improvement, ultimately enabling better decision-making and risk management.

A firm which fully utilizes technology in its VRM processes can make tactical or strategic decisions to scale rapidly with the confidence that any incurred third-party risk is understood, managed, and mitigated by specialized solutions. The increased efficiency and precision of their VRM process will also reduce the underlying operational costs associated with third parties as part of their expansion.

[11] https://www.sai360.com/resources/grc/do-this-not-that-guide-automating-your-vendor-risk-management-program-infographic

Have your cake AND eat it...

In conclusion, effectively managing vendor risk doesn't have to be a burden on your organization's resources or hinder innovation and expansion. By making full use of the latest VRM technologies, you can reap the benefits of outsourcing while minimizing potential risks. In fact, adopting a robust and technology driven VRM framework can lead to competitive advantages that will set your organization apart in the market.

Greater agility and speed

A robust VRM framework allows your organization to act swiftly in response to market changes or opportunities. With comprehensive risk assessments and real-time monitoring in place, you can quickly onboard new vendors or scale operations, capitalizing on first-mover advantages and seizing new market opportunities.

Improved resource allocation

Automation within VRM processes frees up employees to focus on higher-value tasks. By eliminating manual and repetitive work, your team can dedicate more time and energy to strategic initiatives that drive business growth, ultimately leading to increased job satisfaction and reduced employee turnover.

A stronger supply chain

Advanced reporting and analytics provide valuable insights into vendor performance, compliance, and risk levels. This information empowers your organization to make more informed decisions about vendor relationships, improving overall risk management, and strengthening your supply chain.

SAI360's unified approach to risk sets us apart

Today's complex risk landscape demands more. SAI360 leads the way with an integrated GRC platform and Learning solution that spans the entire risk and compliance spectrum.

Risk Management Solutions

- Risk & Compliance Management Solutions
- Enterprise & Operational Risk Management
- Regulatory Compliance
- Policy Management
- Third-Party / Vendor Risk Management
- Internal Controls
- Internal Audit
- Incident Management
- Conflicts of Interest (COI)
- Gifts and Hospitality
- IT & Cybersecurity
- Business Continuity Management

Ethics & Compliance Learning Solutions

- Anti-Bribery & Anti-Corruption
- Competition & Anti-Trust
- Conflicts of Interest
- Data Protection & Privacy
- Exports, Imports & Trade Compliance
- Harassment & Discrimination

SAI360
RISK FROM EVERY ANGLE

SAI360 is giving companies a new perspective on risk management. By integrating Governance, Risk, Compliance (GRC) software and Ethics & Compliance Learning resources, SAI360 can broaden your risk horizon and increase your ability to identify, manage, and mitigate risk. See risk from every angle.
Visit www.sai360.com.