G00299306

Formalize Vendor Risk Management Practices to Lessen the Probability of Business Disruption

Published: 28 September 2016

Analyst(s): Christopher Ambrose

Failure to implement a comprehensive IT vendor risk management program increases the potential for business disruption. IT vendor risk management leaders have a strategic imperative to help their organizations identify, monitor and mitigate risks from IT vendors and service providers.

Key Challenges

- IT vendor risk management leaders battle lack of awareness or disregard of vendor risk management policies and the resulting independent and uncoordinated actions that can lead to operational and business continuity risk events.
- IT vendor risk management responsibilities spread across the organization often lack consistent, integrated practices for identifying, monitoring and mitigating third-party and vendor risks.
- IT vendor risk management leaders bear the responsibility for minimizing business exposure to compliance issues and service disruptions, often with limited resources and authority.

Recommendations

IT vendor risk management leaders should:

- Align your IT vendor risk management program with your information security and enterprise risk management programs.
- Prioritize your most critical vendor risks, and evaluate the capabilities of existing IT vendor risk management controls.
- Implement an IT vendor risk management classification framework that covers all relevant risk planning, identification, monitoring and mitigation activities.

- Execute a risk control action plan that provides for ongoing monitoring and identification of IT vendor risks and that includes an actionable plan to ensure business continuity, security and adequate vendor performance.

Table of Contents

List of Tables

List of Figures

Strategic Planning Assumptions

By 2018, undetected and uncontrolled IT vendor risks will accelerate formal investment in IT vendor risk mitigation programs beyond regulated industries.

By 2018, regulations, cloud adoption and internal mandates will increase the existence of formalized IT vendor risk management programs from approximately 10% of enterprises to 40%.

By 2019, the need for transparency into operational and security activities within a vendor's value network (including subcontractors) will drive demand for vendor security, as well as risk management solutions and services by 30%.

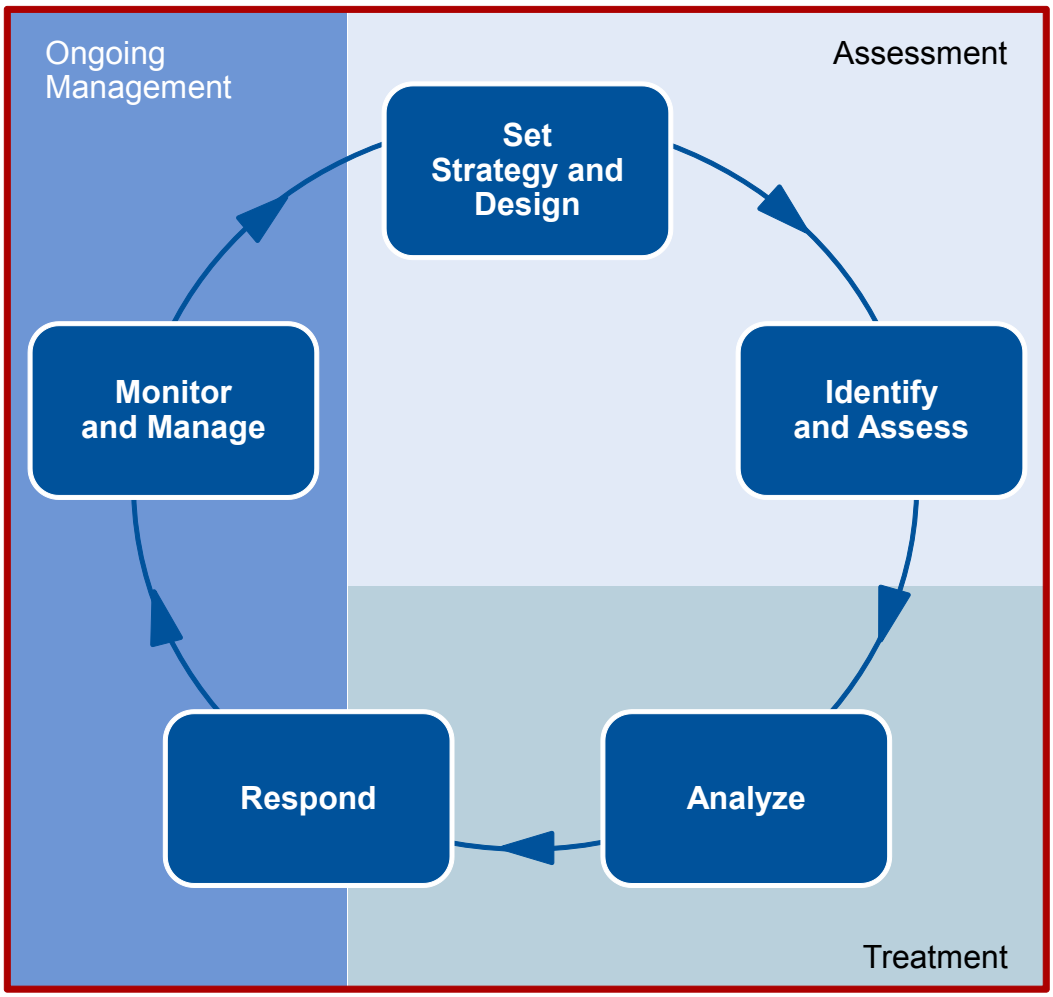
Introduction

Organizations are exposed to a number of risks when they work with vendors and third parties. The move to cloud and software as a service delivery models increases these risks because many cloud service providers (CSPs) haven't consistently showed the same level of operational resilience as traditional outsourcers and service providers. Add to this the often singular reliance on a particular provider delivering a shared service to many customers, and the risk to business operations is evident.[1] Highly regulated industries such as banking, insurance and healthcare are increasingly compelled to manage their vendor risks by stringent regulations and continuous audits.[2] All organizations that work with IT vendors should develop formal IT vendor risk management programs, regardless of regulation, as a best practice for achieving business goals and meeting their missions.

IT vendor risk management (VRM) is the process of ensuring that the use of third-party service providers and IT suppliers does not create an unacceptable potential for business disruption or a negative impact on business performance. It specifically identifies those third parties that are responsible for managing, have access to, or supply data to information assets. It additionally includes third parties that access or control critical business processes and IT systems (see "Hype Cycle for Risk Management Solutions, 2016").

IT vendor risk management should go beyond financial due diligence and security and extend to regulatory, geographic, operational and strategic risks that can impact a vendor's ability to meet its contractual commitments. (See Figure 1 for an example of an IT vendor risk management framework.)

Figure 1. IT Vendor Risk Management Framework



Source: Gartner (September 2016)

Analysis

Align Your IT Vendor Risk Management Program With Your Information Security and Enterprise Risk Management Programs

IT vendor risk management must align with an organization's enterprise, operational and IT risk management programs to ensure end-to-end process continuity and effective risk governance. IT vendor risk management activities are performed within organizational and process boundaries, but should be viewed across the spectrum of risks and risk mitigation strategies. For example:

- Procurement will often perform financial due diligence and may get continuous updates from services like Dun & Bradstreet, which provides vendor credit risk data.

- Information security will look at security controls, certifications like Service Organization Control (SOC) 2 and International Organization for Standardization (ISO) 27001, responses to questionnaires from Shared Assessments or the Cloud Security Alliance, and data privacy controls provided by vendors.
- Legal may review contract clauses and sources for information on pending litigation or the possibility of mergers or acquisitions (see Shared Assessment and Cloud Security Alliance).

These are just some of the organizational and process boundaries for risk identification and monitoring. Too often, when it comes to indirect spending categories like IT, there is no single authority, accountability or responsibility for all IT vendor risk management controls.

An IT vendor risk management plan that aligns to the enterprise risk management plan can:

- Provide the foundation for ensuring supplier business continuity management (BCM) and contingency planning
- Link information security risks and financial viability risks
- Identify the governance requirements for developing transparency and visibility into the IT supply chain[3]

Prioritize Critical Vendor Risks Based on Their Business Impacts

There are many sources for identifying the types and classes of risks. Risks can be grouped by their impact to a company, an organization, an initiative, a government agency or an agency mission. These risks generally fall into the following areas:

Financial risk identifies the financial viability of a vendor and the likelihood of whether the vendor is currently experiencing or will experience any financial issues that will impair its ability to fulfill its obligations to its customers. Financial risk is typically assessed upfront in the due diligence phase of vendor selection and contract negotiation. Many factors and forces can affect the financial risk of a vendor, including market dynamics, economic climate, competition, and vendor operational and business models.

Operational risk identifies the risk to an organization's ability to operate its key business functions due to a failure by a vendor to perform all or part of that business function. This can result from a vendor's failure to provide adequate resourcing, deficient processes and a vendor's ability to respond to external factors. This should also include an assessment of the vendor's BCM program and IT disaster recovery plan, with strong focus on the vendor's ability to recover from interruptions to the supply of services in accordance with your own recovery requirements. Such interruptions include technology failure, civil unrest and natural disasters.

Regulatory and compliance risk examines a range of regulatory, industry, process and geographic requirements that vendors must comply with and that clients have to assess and track. These risks can be related to many different areas, including accounting, reporting, usage rights, data privacy and security, recovery and continuity. Failure of the organization to adequately assess and track

these factors could lead to criminal or civil penalties, enforceable undertakings and an impact on the enterprise's ability to conduct business.

Strategy risk analyzes the risk associated with vendors changing their strategy in relation to the products or services that a client has acquired. Abrupt strategy changes, or failure to adapt to a strategy change, can lead to vendors exiting a market, altering a product or solution, or failing to keep pace with customer, technology or market changes. This may also include changing the vendor's supply chain and subcontractors, which may often be the result of changes in executive management.

Geographic risk identifies the risks primarily with services or product delivery occurring in countries or regions other than the client's home country or region. These risks could be geopolitical, or they could be driven by climate or natural disaster, currency fluctuations, legal, resource, or infrastructure-related risks.

Risks can further be broken down into how they can affect your operations and your business. Identifying, monitoring and remediating risks require an enterprise to have a clear understanding of potential risks and their overall impact to the business. IT vendor risk management leaders should periodically assess their vendor risk management strategy and capabilities across risk categories.

Gartner has compiled a list of 10 specific vendor risks and their potential impacts in Figure 2. These risks can impact and influence many, if not all, of the identified risk classes above.

Figure 2. Vendor Risks

Risk Class	Vendor Risks	Customer Impacts
Financial	Viability, short and long term	Reputation Brand Revenue Profitability Growth Survival
	Stability	
Operational	Performance and ability to maintain service levels	
	Cyber and infosec, physical	
Compliance	Regulatory requirements	
	Legal	
Strategic	Leadership changes	
	Strategy changes	
Geographic	Geopolitical and structural	
	Currency fluctuations	

Source: Gartner (September 2016)

Due diligence and ongoing monitoring should be used to address these risks. Also, contingency plans should be developed for all critical vendors, but with the realization that some plans may be impractical to actually enact. This means greater monitoring and early detection are vital. A risk register should be created to collect and report on these risks as well. With cloud computing and software-as-a-service adoption increasing, fourth-party and subcontractor risk will continue to

increase in importance. (See "Toolkit: Sample IT Risk Register" and "Toolkit: Interactive Sourcing Risk Register.") Many regulatory bodies have identified fourth-party relationships with third parties as a critical risk. They are providing guidance that companies should at the very least have some visibility and transparency into understanding their vendors' supply chains as well as understanding how their third parties are ensuring that all relevant risks with fourth parties are addressed.[4]

Implement an IT Vendor Risk Management Classification Framework

Determining which vendors need more rigorous assessments requires the development of a vendor risk tier system. A tier system identifies the type of risk, the likelihood of its occurrence, its impact and the approach to risk mitigation. (See "How to Evaluate Cloud Service Provider Security.") The chance of a risk occurring could be defined as highly likely or unlikely to occur. Impact can be measured in terms of financial exposure, impact to operations, reputation and brand image.

Organizations classify or categorize vendors for a number of purposes. Sourcing and procurement organizations create classifications to segment suppliers by spend category (for example, hardware, software and services). They also segment them based on their strategic value to the business. For risk and security purposes, classification is used to identify the suppliers that have access or control over data, processes or systems. The criteria for classifying and tiers can include the following:[5]

Mission-critical: The supplier supports or performs a vital core function that is critical to your organization's survival. If this function were unavailable, there would be a threat to the organization's ability to stay in operation, leading to irreparable damage (for example, failure to meet financial obligations for clients or itself or generating a major impact to personnel or public life/safety). This also needs to evaluate a combination of the criticality of the process, and the degree to which success was dependent upon supplier execution?

Critical: The supplier supports a critical function that is important to maintain the operations of the organization. If this function were to be unavailable, there would be a significant impact to the organization resulting in:

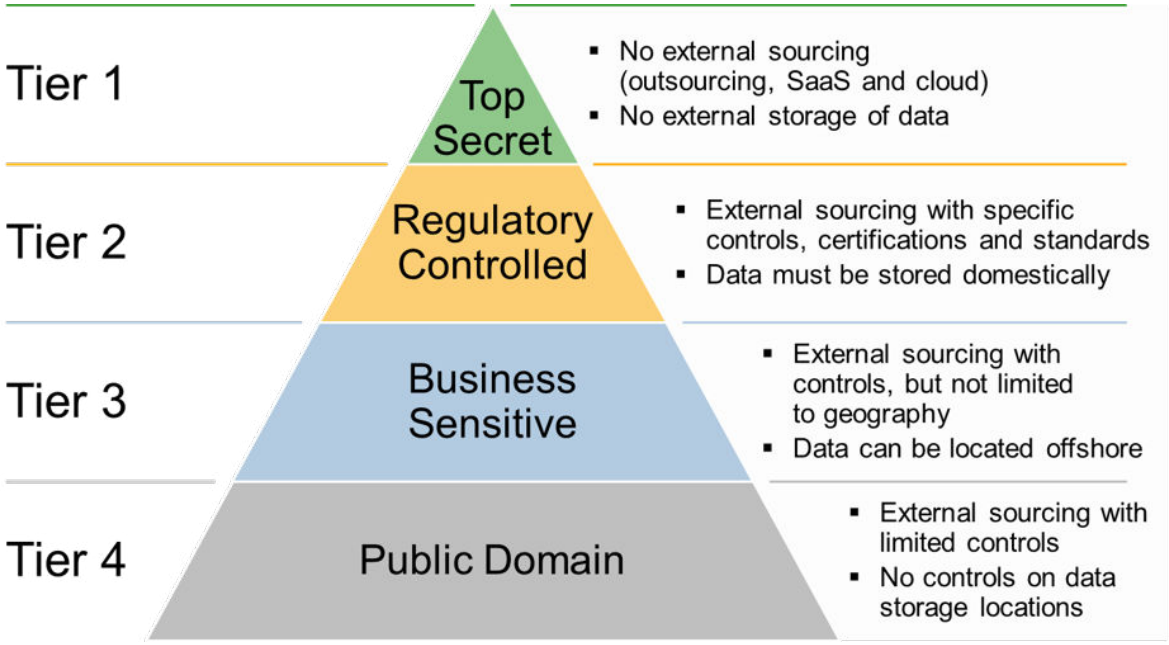
- A regulatory breach
- Financial or reputational loss leading to potential major liquidity problems
- Widespread negative press coverage leading to loss of clients or market share
- Severe disruption of a regional strategy

Important: The supplier supports a function that is involved in the ongoing operation of the organization. If this function were to be unavailable, there would be a moderate impact on the organization, potentially resulting in a regulatory breach, a nonmaterial financial or reputational loss, limited media coverage or the disruption of a local strategy.

Deferrable: The supplier supports a function that is noncritical to the organization. If this function were to be unavailable, there would be an insignificant impact to the organization.

However, to deal with security risks, a second approach to classifying vendors is needed. This approach looks at data classification as well as system or process classification. Data classes for security and risk management purposes are often tiered depending on data criticality and sensitivity (see Figure 3). The highest tier of data may be determined to be data that is the "secret sauce" of the business: intellectual property, formulas, unique business secrets and classified government information, for example. A second tier of data could be critical customer and employee data to include social security numbers, PCI and protected health information (PHI) data. A third tier of data could include sensitive business data related to sales forecasts, profitability, nonidentified customer information and analytics. A fourth tier could be data that is also in the public domain. A set of controls and requirements is then placed on the vendors to be managed, often by the information security organization within an enterprise. The guidance for sourcing and data storage are provided as examples and may vary within your organization.

Figure 3. Data Classification Vendor Tiers — Example



Source: Gartner (September 2016)

Regardless of the data classification and tiering model, an assessment of impact should also be performed. There are three business goals of maintaining confidentiality, maintaining integrity and maintaining availability. Some organizations may choose to have other business goals, such as nonrepudiation or regulatory compliance, but the wider information security community has no agreement on what additional goals would be. An impact scale provides a hierarchical set of levels that are used to estimate anticipated level of loss, damage, or other form of impact that would result if some sort of failure or incident resulted in a failure to meet one of the business objectives. It is a mechanism to estimate the potential business impact so that an appropriate decision can be made for further risk assessment, thus leading to a decision to accept, mitigate, transfer or avoid a specific risk situation. Policies force the line of business and IT to agree on and use a classification scheme, which is supported by processes, and possibly automation, to ensure a reliable and

efficient follow-through. For a more in-depth discussion of data classification, see "Toolkit: Creating Data Classification Schemes." See Figure 3 for an example of the impact scale.

Table 1. Impact Levels

	Data Sensitivity		
Forms of Impact	**Low**	**Moderate**	**High**
Monetary loss	Up to $10,000	$10,000 to $1 million loss	More than $1 million loss
Human loss	No medical attention	Injury requiring hospitalization	Death
Customer defection	More than 1% of accounts	2% to 5% of accounts	More than 5% of accounts
Market Share	No reduction	1% to 3% reduction	More than 4% reduction
Privacy breach	Less than 100 records	100 to 3,000 records	More than 3,000 records
Competitive breach	No measurable loss	$10,000 to $1 million loss	More than $1 million loss

Source: Gartner (September 2016)

Implement Your Risk Control Action Plan

Once the risk framework and the risk classification is complete, the process of monitoring and mitigating risks should begin. Our research shows that, in most cases, a risk assessment is performed prior to contracting, with limited monitoring of financial viability and information security practices (see "Developing Your SaaS Governance Framework"). Monitoring and ongoing risk mitigation should include:

- Establishment of an oversight and governance body that looks across all risk areas and impacted organizational and business units to ensure a unified approach to IT vendor risk management.
- The development and ongoing review of an IT vendor risk register. The vendor risk register should at a minimum identify the risks, the responsible organization, the potential risk impact and what mitigation efforts are being undertaken.
- The evaluation of an IT vendor risk management tool that provides for risk tracking, risk profiling, risk assessment and risk monitoring (see "Magic Quadrant for IT Vendor Risk Management").
- Regular reviews with key stakeholders from the business, sourcing, vendor management, legal, IT, enterprise risk management and information security. These reviews should examine current and future risks and identify any gaps in IT vendor risk management policies or processes.

IT vendor risk management is recognized by a number of regulatory bodies and standards organizations as a much-needed critical business discipline. As more organizations become more

reliant on third parties to support and deliver critical IT and business processes, the potential number of points of failure continues to increase. Vendors are now viewed by many as part of an ecosystem of internal and external supply, and the management of vendor risks is considered at the same level of criticality as managing internal business risks.

Case Study

A services company needed to develop a comprehensive program for identifying and managing its IT vendor and service provider risks. Historically, the IT security department conducted security risk assessments, but only after being made aware that a potential risk existed with a vendor that was being evaluated in the acquisition process. The process was incomplete. Business units could bypass risk, security, and the procurement organization, often if the contract spend level was below a predefined threshold. The company implemented a framework for identifying clearer criteria whereby a vendor would be required to have its risks assessed and analyzed prior to the completion of a contract.

This process worked most of the time, but business units viewed it as inefficient and often were too willing to knowingly or unknowingly accept a range of risks. To counteract this bypass, the company implemented several measures:

- It eliminated the spending threshold for security reviews and assessments. To streamline the process, it instituted a "triage" approach, requiring the business to answer a relatively small number of security-related questions on all new vendor contracts before signing. Dependent on the answers, varying degrees of risk assessment and analysis were then performed, and the business was informed of the level of risk.
- The procurement department was made responsible for coordinating the risk process (not completing the risk assessments) because it was often the point of entry for all new vendor contracts.
- Executive management was continually updated on risk policies, and senior executives were given the responsibility to ensure that the vendor risk process was adhered to within their organizations. Regular risk review meetings were conducted to ensure this was occurring.
- A review process for existing contracts was created so that previously nonassessed vendors and contracts could be put into a review cycle, often coinciding with their renewal dates (unless a review was required sooner).

The results were the effective implementation of better risk identification and risk reviews as well as better-educated business units that understood the potential risks and impacts for their vendor and service acquisition decisions.

Gartner Recommended Reading

Some documents may not be available as part of your current Gartner subscription.

"Develop Contingency Plans for Your Critical Suppliers, or Risk Business Disruption"

"Monitor Key Risk Criteria to Mitigate Vendor Failure"

"Magic Quadrant for IT Vendor Risk Management"

"Cloud Contracts Need Security Service Levels to Better Manage Risk"

"Toolkit: Interactive Sourcing Risk Register"

"Toolkit: Create and Implement a Sourcing Risk Management Framework"

"How to Evaluate Cloud Service Provider Security"

"A Public Cloud Risk Model: Accepting Cloud Risk Is OK, Ignoring Cloud Risk Is Tragic"

Evidence

[1] Gartner analysts have seen a 25% increase in client interactions on the challenges of vendor risk management from 2015 to 2016.

[2] "Risk Management Guidance," Office of the Comptroller of the Currency.

[3] "COBIT 5 Vendor Management Control Objectives for Vendor Management," ISACA.

[4] "NIST Special Publication 800-161: Supply Chain Risk Management Practices for Federal Information Systems and Organizations," National Institute of Standards and Technology.

[5] "Business Continuity Planning: Appendix J: Strengthening the Resilience of Outsourced Technology Services," Federal Financial Institutions Examination Council.

GARTNER HEADQUARTERS

Corporate Headquarters
56 Top Gallant Road
Stamford, CT 06902-7700
USA
+1 203 964 0096

Regional Headquarters
AUSTRALIA
BRAZIL
JAPAN
UNITED KINGDOM

For a complete list of worldwide locations,
visit http://www.gartner.com/technology/about.jsp