Banyan
Business Outcomes LLC

Managing 3rd Party Risk

By Dr. Linda Kostic &
Steven Nichols, MBA
Banyan Business Outcomes LLC

Technology vendors and other 3rd parties create leverage, flexibility, and scale for their clients. They are an essential part of how businesses operate and create stakeholder value. These vendor relationships, however, also increase the risk of an interruption in service, exposure of corporate data, ransomware attack, or other impactful event.

While it's not possible to eliminate 3rd party risk, it is possible to manage it through a combination of sourcing best practices, contractual terms, governance, and collaboration. Companies need to understand the risk presented by 3rd parties and develop an appropriate risk management program.

Managing Risk Through Sourcing

Vendor sourcing efforts should be contextualized with the company's risk profile (the likelihood and severity of risks facing the company) and risk appetite (the level of residual risk that the organization is willing to accept.) The question is, how much risk is acceptable, and is the level of uncontrollable risk presented by the service within that acceptable range?

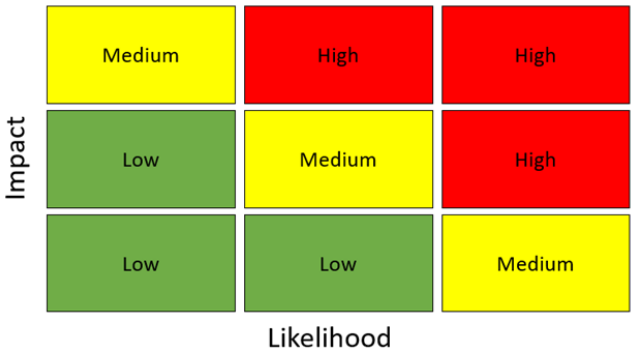
Not every vendor risk profile will justify a full risk assessment[i]. Risk mitigation efforts should be commensurate with the level of risk presented by the service.[ii] For some 3rd party services, a full approach as outlined below may make sense.

Step 1. Identify inherent risks associated with the engagement

What could go wrong? It's a question about the hypothetical scenarios that could create an adverse event for the client. Could project failure create an operational impact? Will the vendor performing the service have credentials that could be used to inject ransomware? Could human error or a 3rd party outage create a problem?

Step 2. Rate the inherent risks

Rate each risk by its likelihood and impact. Determine if there are significant risks that require a full risk assessment. For high/medium risks, identify required controls and identify required contract elements.



COBIT 2019 management objectives EDM03 Ensured Risk Optimization and APO12 Managed Risk provide structure and context for any 3rd party risk assessment. The IT Risk Framework is also an excellent resource.

3. Evaluate control effectiveness through evidence provided by the supplier

Work with the supplier to manage the risk by putting in place effective controls with a known history of success. Suppliers should be able to talk to password management, for example, or their project management practices. These controls reduce the probability and impact of the risk.

If the service or vendor in question presents moderate or high levels of risk, vendors should be required to prove their ability to manage that risk through certifications and audits. Some examples are:

- Risk IT Framework (ISACA) – risk assessments for outsourcing engagements can align with the internally considered risks and controls.[iii]
- Statements on Standards for Attestation Engagements (SSAE)[iv] – An auditing standard by the AICPA that service organizations can use to demonstrate their effectiveness cybersecurity internal controls.
- ISO 27001[v] – Global standard for demonstrating effectiveness of information security management systems.
- NIST[vi] – NIST offers a set of best practices for cybersecurity and risk management (specifically NISTIR 8286)
- SIG[vii] - SIG is a standard questionnaire vendors can fill out to demonstrate their approach to security.

Step 4. Calculate the residual risk and compare it against risk profile

Some risks remain after controls and contracts have been put into place. Compare that level of risk with the risk profile[viii] to determine if the controls are sufficient.

Contractual Terms and Risk

While companies cannot fully eliminate risk through strong contract language, they can reduce it and establish legal remedies. Qualified legal counsel should be consulted whenever committing to a

relationship that creates risk. Here are a few risk-related terms to watch for in agreements given certain risk profiles.

Compliance & Auditing

3rd parties which committed to certain controls and certifications during the sourcing process should be required to maintain that level of certification. If the RFP stipulated ISO27001, SOC Type 2, or some other certification, that certification should be maintained.

The client should have the ability to audit vendor adherence to security controls either through a 3rd party or directly. For example, if vendors have corporate email addresses or network access, they should be subject to the same phish testing policies as the rest of the organization.

Ransomware groups have identified technology managed services providers as especially rich targets for their efforts, as many of these companies have access to their clients' networks. 3rd parties are a common vector for cybersecurity incidents.

Timely Reporting

In the event that a cybersecurity incident exposes client data or creates a risk for clients, the 3rd party should be obligated to immediately disclose the event to the client.

Legal Remedies

The impact of a cybersecurity incident can be disproportionate to the fees paid to the vendor. Cybersecurity incidents can damage the client's reputation, jeopardize their strategic position, interrupt revenues, and create substantial hard costs. These costs should be recoverable from the vendor to the extent that the vendor is accountable for the incident.

Insurance

Business insurance protects the vendor from substantial losses and creates a sort of bond the client can use to recover from losses.

Fourth Parties/Subcontractors

If the firm permits 4th parties/subcontractors, indicate that the third-party conducts risk assessments and provides continuous oversight.

3rd Party Risk & Governance

After a vendor has been sourced and the contract signed, the internal and 3rd party delivery teams begin working together. The norms and behaviors of these teams will largely determine whether the risks are realized. Companies should build a governance structure to ensure a strong relationship based on open communication and collaboration.

Many of the hard-fought terms and conditions, service level agreements (SLAs), Key Performance Indicators (KPIs), and other obligations that were discussed during the sales process and recorded during contracting can be quickly forgotten when operational pressure is applied. Governance is a process for ensuring these requirements are met and the relationship continues to grow as planned.

Banyan
Business Outcomes LLC

Risk is an essential part of vendor governance. Vendor commitments relative to risk should be reviewed regularly by operational and leadership teams.

- **Project meetings** – Every project update should include a section on how to improve the security posture of the extended enterprise. Security standards shouldn't be compromised even if teams are stretched thin or required to rush.
- **Weekly/Monthly Operational Reviews** – Operational teams should prioritize delivery of any required security-related deliverables or performance. Every ticket, deliverable, change, action, or behavior should be completed with an eye toward cybersecurity. That emphasis should be evident in the way those actions are reported in the weekly meeting.
- **Quarterly Business Reviews (QBRs)** – Typically more strategic in nature, QBRs are an opportunity for leadership to emphasize the importance of cybersecurity. They are also an opportunity for the vendor to differentiate themselves by promoting their cybersecurity advancements and investments. Typically, cybersecurity should be a separate item on the agenda.

Collaboration for Managed 3rd Party Risk

Open and honest conversations across the corporate boundary are the strongest defense against Cybersecurity incidents and risk. Casual dialogues keep the issue top of mind and go a long way toward preventing a momentary lapse that creates an opening.

- *"Did you hear about that cybersecurity breach?"*
- *"Did you see this article?"*
- *"How could we do better?"*

3rd party risk is a shared responsibility that requires the right sourcing process, contract terms, governance and relationship. By prioritizing this risk, companies can reduce their exposure and the likelihood of an incident that ends up in the court room.

---

[i] COBIT 2019 Management Practice APO12.03
[ii] https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html
[iii] https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9WEAS
[iv] https://us.aicpa.org/research/standards/auditattest/ssae
[v] https://www.iso.org/isoiec-27001-information-security.html
[vi] https://www.nist.gov/risk-management
[vii] https://sharedassessments.org/sig/
[viii] https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004Ko9VEAS