Vendor Risk Category Resource

While the following list of questions is not exhaustive, the questions can be used to encourage conversation when evaluating each of the risk categories. Learn more about how Tandem can help you conduct vendor risk assessments at https://tandem.app/vendor-management-software.

Strategic Risk

- Does implementing this vendor service align with the organization's mission?
- Will your vendor oversight periodically reevaluate this vendor's ability to reflect the organization's mission?

Reputation Risk

- Has this vendor or individuals representing this vendor previously been involved in a controversial public matter which could cause unwanted attention for the organization?
- Is this vendor or individuals representing this vendor in a field of public interest (e.g., social, religious, politics, etc.) which could cause unwanted attention for the organization?
- Does this vendor have an acceptable use policy which disallows employees from unauthorized disclosure about the organization?
- Does the organization have a non-disclosure agreement with this vendor?
- Does this vendor use subcontractors to provide this service and if so, has the vendor conducted adequate due diligence?

Operational Risk

Operational risk can be thought of as the possibility of vendor inadequacy or failure and the potential effect on daily operations.

- How much experience does this vendor have providing this service?
- Does this vendor use subcontractors to provide this service and if so, has the vendor conducted adequate due diligence?
- Does this vendor maintain adequate staffing to perform this service?
- Has this vendor evaluated the possibility of unforeseen events and verified plans to maintain operations (e.g., business continuity planning and testing)?
- Can the organization validate this vendor’s operational and security practices have been independently verified (e.g., SOC reports, security testing, etc.)?

Transaction Risk

Transaction risk can be thought of as the reality of vendor inadequacy or failure and the consequential effect on the ability to process transactions.

- Does this vendor have an Information Security Officer and Information Security Program?
- Does this vendor use subcontractors to provide this service and if so, has the vendor conducted adequate due diligence?
- In the event of unforeseen events occurring, does this vendor have adequate plans to correct any issues and prevent the issues from happening again (e.g., incident response plan)?
- Do contracts or other service agreements with this vendor protect the organization by addressing performance, liability, confidentiality, and insurance requirements?

Credit Risk

- Can the organization validate this vendor is financially stable?
- Does the organization have a clear understanding regarding the products and services this vendor will provide?

Compliance and Legal Risk

- Does the contract address this vendor's expected compliance with applicable law, regulation, and guidance?
- Is this vendor or any of this vendor's subcontractors considered a foreign-based service provider?
- Does this vendor have an Information Security Officer and Information Security Program?
- Does the organization periodically have an independent validation (e.g., audit, compliance review, etc.) of the vendor management program?

Other Risk

- Are there risks the organization has considered which have not been addressed by any other category?