

# Third-Party Risk Assessment Checklist

Vendors that are or will be critical dependencies in a company’s value chain should receive an appropriate level of scrutiny before being engaged. Here are a series of questions to ask these vendors to assess what level of risk they may pose to your business operations.

## How to use this document

1. Identify your business’s mission-essential functions and processes
2. Identify which mission-essential functions are performed or enabled by a third-party product or service
3. Identify which third-party products or services don’t have existing or easily-sourced alternatives
4. For each of the third-party products or services in your list, answer the below questions

At-Bay cyber insurance policyholders may have access to At-Bay Stance Advisory Services\*. This is a team of advisors who can help review your third-party risk assessment, identify your risk, and discuss recommendations.

[Schedule a call](#) with At-Bay’s Advisory Services team for your assessment.

MISSION-ESSENTIAL FUNCTIONS	PRODUCT OR SERVICE THAT ENABLES THE MISSION-ESSENTIAL FUNCTION	IS THERE AN EASILY-SOURCED ALTERNATIVE?
EXAMPLE Insurance Claim Processing	Change Healthcare	<input type="checkbox"/> YES <input type="checkbox"/> NO
		<input type="checkbox"/> YES <input type="checkbox"/> NO
		<input type="checkbox"/> YES <input type="checkbox"/> NO
		<input type="checkbox"/> YES <input type="checkbox"/> NO
		<input type="checkbox"/> YES <input type="checkbox"/> NO
		<input type="checkbox"/> YES <input type="checkbox"/> NO

MAKE A COPY OF THIS WORKSHEET FOR EACH MISSION-ESSENTIAL VENDOR

QUESTIONS	NOTES
<p>Does the vendor have industry-standard security controls in place?</p>	
<p>Does the vendor appear to have conducted their own contingency planning sufficient to make them resilient to attack?</p>	
<p>Is the vendor aware of their legal and contractual obligations to customers for cybersecurity?</p>	
<p>Does the vendor have one or more industry certifications such as SOC 2, HITRUST, etc.?</p>	
<p>Do we have a clear understanding of what data we share with this vendor?</p>	
<p>Do we have a clear understanding of any technology integrations or access that we share with this vendor?</p>	
<p>Have we identified alternatives to this vendor if / when they become necessary?</p>	
<p>What is the impact to our organization if this vendor experiences a security failure or outage?</p>	
<p>What are the legal implications to us and our stakeholders of a security failure or outage with this vendor?</p>	
<p>What recourse do we have in the event of a security failure or outage with this vendor?</p>	

---

# About Third-Party Risk for Businesses

Third-party risks are the risks to a business stemming from anything that a supplier, vendor, customer, or business partner does or fails to do.

Third-party risks aren't new. But, the increasing reliance by businesses on technology products and services from other companies is. [At-Bay's 2024 InsurSec Report](#) found Indirect Ransomware (an incident where an organization is indirectly impacted by a cyber event on their vendor or partner) exploded by 415% in 2023.

This situation has led to increased risk for businesses and warrants an assessment and understanding of such risks as part of ongoing business continuity planning and risk management procedures.

## About At-Bay

At-Bay is the InsurSec provider for the digital age. By combining world-class technology with industry-leading insurance and security expertise, At-Bay was designed from the ground up to empower businesses of every size to meet cyber risk head on.

The At-Bay Group includes a cybersecurity company and a full-stack insurance company. As an insurance company, At-Bay offers Cyber, Tech E&O, and Miscellaneous Professional Liability policies.

Our InsurSec approach provides end-to-end protection for modern businesses. It's a force multiplier that includes security, threat intelligence, and human experts to close the SMB cybersecurity gap – all as part of their insurance policy.

---

\* Access to At-Bay Stance Advisory Services is available to policyholders via the "Embedded Security" fee and the corresponding endorsement. Your Embedded Security Endorsement refers to "At-Bay Stance Advisory Services" as "At-Bay Stance Managed Security.