Risk Type	Potential Actions*	High Risk	Medium Risk	Low Risk	All Vendors
Operational Disruption of Services High – Disruption of service affects State operations within one business day Medium – Disruption of service affects State operations within 2-5 business days Low – Disruption of service affects State operations beyond a 5-day loss of service	Ensure appropriate contractual safeguards based on risk assessment of services				X
	Conduct site visits based on specific triggers/risks (i.e., when warranted)	X	X Consider virtual		
	Review and assess business continuity program and the related test results. Contract should require reporting of test results and notice of when plan is invoked	X Annually			
	Require third party reviews of relevant vendor policies and controls, with reports provided to the State	X	X		
	Certifications to be signed by an officer of the vendor	X Quarterly	X Annually		
	Formal meetings with vendor that include appropriate State Staff	X Monthly	X Quarterly		
	Consider requiring background checks/bonding requirements for key employees if warranted due to employee access concerns or other significant employee risks/exposures	X	X		
	Consider potential vendors' risk mitigation efforts with respect to work-from-home policies and associated access/software update concerns.	X	X		
Reputational High: Negative financial or other information about vendor likely would undermine confidence in the administration, oversight, or operation of a Plan Medium: Negative information about vendor could undermine confidence Low: Negative information about vendor not likely to undermine confidence	Establish automatic alerts for news and financial reporting items and assign an employee to monitor within one day of publication				X
	Monitor industry, recruitment, and other sites that would include survey results, testimonials, and rankings	X			
	Consider potential vendors' risk mitigation efforts with respect to reputational issues, e.g., cybersecurity and business continuity plans. Work-from-home policies and associated access/software update concerns.				
Legal High: Breach could result in third-party claims of more than $1 million Medium: Breach could result in third-party claims of more than $100,000 but less than $1 million Low: Breach not likely to result in third-party claims of more than $100,000	Ongoing monitoring of compliance with contract terms and plan requirements, including SLAs, performance metrics, and billing rates	X Monthly/ Quarterly	X Every six months		
	Monitor case law and litigation activity	X Monthly or as needed			
	Undergo a legal review with the DAG to ensure compliance with relevant Delaware laws, regulations, and Board and OST policies				X
	Vendor contracts shall contain provisions for terminating a vendor relationship and transitioning the services to a successor, including provisions dealing with the return of data and other State property				X

*The list of Potential Actions serves as a guide. OST has the discretion to take the actions it deems appropriate given the specific facts and circumstances of each vendor relationship.