

# Third Party Risk Management

Seagate® works with several types of third parties, and we acknowledge that third-party vendors and suppliers are an essential part of our overall success, providing the most innovative solutions at the best value. However, no matter the industry, third parties have the potential to introduce risks to supply, operations, and/or data.

For example, a partner could suffer a cyber-attack and confidential information could be compromised. Or a supplier of an essential part could suffer a disruption (flood, bankruptcy, viral outbreak) that could impact the supplies needed to continue manufacturing products for end customers.

Thus, **Seagate has instituted a robust third-party risk management program** that emphasizes risk assessment, due diligence, monitoring, and reporting. We have dedicated resources on numerous teams to continuously manage the risks posed by third parties.



Seagate maintains constant communication with our third parties that includes real time monitoring and alerting of impactful events, regular risk assessments, analysis, and treatment of any risk associated with third parties, as well as numerous other processes. This work is continually evolving to keep pace with emerging risk factors.

In conclusion, Seagate recognizes that the world is constantly changing—from global trade regulations to intensifying storms to geopolitical conflicts—and new risks are evolving. Managing these risks is crucial to the reliability of our business. That’s why Seagate has implemented a comprehensive and proactive risk management strategy that mitigates risk exposure across our supply chain. **Our approach to third-party risk management demonstrates our commitment and vigilance towards safeguarding operations, assets, and customers’ data.**